pi-hole / docker-pi-hole Public

Code Issues 30 Pull requests 4 Discussions Actions Projects 1 Security Insights

master Go to file Code

yubiuser Merge pull request #1472 from pi-hole/tweak/de... ··· ✓ on Oct 31 **1,655**

.github	Add pip ecosystem to dependabot	last month
examples	Replace deprecated variables with the correct ...	9 months ago
src	Fixed spellcheck.	last month
test	Only allow https for curl	7 months ago
.codespellignore	add padd to .codespellignore.	last year
.gitignore	use docker-compose example yaml	3 years ago
.gitmodules	remove submodules	7 years ago
CHANGELOG.md	Couple of typos in docs.	2 years ago
CONTRIBUTING.md	fixed broken link to TESTING.md	last year
LICENSE	add EUPL license	3 months ago
README.md	adminLTE->web	last month
build-and-test.sh	Enable colors for pytest output. This certainly ...	10 months ago

About

Pi-hole in a docker container

pi-hole.net

#dns #docker-container #web-app #pi-hole #ad-blocker

Readme

View license

Code of conduct

Security policy

Activity

7.2k stars

100 watching

1.1k forks

Report repository

Releases 96

2023.11.0 Latest
last week

README.md

Docker Pi-hole

Upgrade Notes

- **Using Watchtower? See the Note on Watchtower at the bottom of this readme**
- As of `2023.01`, if you have any modifications for lighttpd via an `external.conf` file, this file now needs to be mapped into `/etc/lighttpd/conf-enabled/whateverfile.conf` instead
- Due to a known issue with Docker and libseccomp <2.5, you may run into issues running `2022.04` and later on host systems with an older version of `libseccomp2` (Such as Debian/Raspbian buster or Ubuntu 20.04, and maybe CentOS 7).

  The first recommendation is to upgrade your host OS, which will include a more up to date (and fixed) version of `libseccomp`.

+ 95 releases

Sponsor this project

pi-hole Pi-hole

https://pi-hole.net/donate

patreon.com/**pihole**

Learn more about GitHub Sponsors

Packages 1

pihole

Contributors 128

+ 114 contributors

Languages

If you absolutely cannot do this, some users have reported success in updating `libseccomp2` via backports on debian, or similar via updates on Ubuntu. You can try this workaround at your own risk (Note, you may also find that you need the latest `docker.io` (more details here)

- Some users have reported issues with using the `--privileged` flag on `2022.04` and above. TL;DR, don't use that mode, and be explicit with the permitted caps (if needed) instead

● **Shell** 62.9% ● **Python** 33.6%
● **Dockerfile** 3.5%

Quick Start

1. Copy docker-compose.yml.example to docker-compose.yml and update as needed. See example below: Docker-compose example:

```
version: "3"

# More info at https://github.com/pi-hole/docker-pi-hole/ and https://doc
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    # For DHCP it is recommended to remove these ports and instead add: r
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "67:67/udp" # Only required if you are using Pi-hole as your DHCP
      - "80:80/tcp"
    environment:
      TZ: 'America/Chicago'
      # WEBPASSWORD: 'set a secure password here or it will be random'
    # Volumes store your data between container upgrades
    volumes:
      - './etc-pihole:/etc/pihole'
      - './etc-dnsmasq.d:/etc/dnsmasq.d'
    #   https://github.com/pi-hole/docker-pi-hole#note-on-capabilities
    cap_add:
      - NET_ADMIN # Required if you are using Pi-hole as your DHCP server
    restart: unless-stopped
```

2. Run `docker compose up -d` to build and start pi-hole (Syntax may be `docker-compose` on older systems)
3. Use the Pi-hole web UI to change the DNS settings *Interface listening behavior* to "Listen on all interfaces, permit all origins", if using Docker's default `bridge` network setting. (This can also be achieved by setting the environment variable `DNSMASQ_LISTENING` to `all`)

Here is an equivalent docker run script.

Overview

A Docker project to make a lightweight x86 and ARM container with Pi-hole functionality.

1. Install docker for your x86-64 system or ARMv7 system using those links. Docker-compose is also recommended.
2. Use the above quick start example, customize if desired.
3. Enjoy!

Test & Build passing docker stars 2.4k docker pulls 828M

Running Pi-hole Docker

This container uses 2 popular ports, port 53 and port 80, so **may conflict with existing applications ports**. If you have no other services or docker containers using port 53/80 (if you do, keep reading below for a reverse proxy example), the minimum arguments required to run this container are in the script docker_run.sh

If you're using a Red Hat based distribution with an SELinux Enforcing policy add `:z` to line with volumes like so:

```
    -v "$(pwd)/etc-pihole:/etc/pihole:z" \
    -v "$(pwd)/etc-dnsmasq.d:/etc/dnsmasq.d:z" \
```

Volumes are recommended for persisting data across container re-creations for updating images. The IP lookup variables may not work for everyone, please review their values and hard code IP and IPv6 if necessary.

You can customize where to store persistent data by setting the `PIHOLE_BASE` environment variable when invoking `docker_run.sh` (e.g. `PIHOLE_BASE=/opt/pihole-storage ./docker_run.sh`). If `PIHOLE_BASE` is not set, files are stored in your current directory when you invoke the script.

Automatic Ad List Updates - since the 3.0+ release, `cron` is baked into the container and will grab the newest versions of your lists and flush your logs. **Set your TZ** environment variable to make sure the midnight log rotation syncs up with your timezone's midnight.

Running DHCP from Docker Pi-Hole

There are multiple different ways to run DHCP from within your Docker Pi-hole container but it is slightly more advanced and one size does not fit all. DHCP and Docker's multiple network modes are covered in detail on our docs site: Docker DHCP and Network Modes

Environment Variables

There are other environment variables if you want to customize various things inside the docker container:

Recommended Variables

Variable	Default	Value	Description
`TZ`	UTC	`<Timezone>`	Set your timezone to make sure logs rotate at local midnight instead of at UTC midnight.
`WEBPASSWORD`	random	`<Admin password>`	http://pi.hole/admin password. Run `docker logs pihole | grep random` to find your random pass.
`FTLCONF_LOCAL_IPV4`	unset	`<Host's IP>`	Set to your server's LAN IP, used by web block modes.

Optional Variables

Variable	Default	Value	
`PIHOLE_DNS_`	`8.8.8.8;8.8.4.4`	IPs delimited by `;`	Upstrear hole to fi separate (support with `#[p` `127.0.0` (support [and links](#) `upstrear` `upstrear` the servi docker s Note: Th environr this as th upstrear added vi be overw restart/r
`DNSSEC`	`false`	`<"true"|"false">`	Enable D
`DNS_BOGUS_PRIV`	`true`	`<"true"|"false">`	Never fo for priva
`DNS_FQDN_REQUIRED`	`true`	`<"true"|"false">`	Never fo
`REV_SERVER`	`false`	`<"true"|"false">`	Enable D forwardi

Variable	Default	Value	
			resolutio
`REV_SERVER_DOMAIN`	unset	Network Domain	If condit enabled, local net
`REV_SERVER_TARGET`	unset	Router's IP	If condit enabled, network
`REV_SERVER_CIDR`	unset	Reverse DNS	If condit enabled, zone (e.g
`DHCP_ACTIVE`	`false`	`<"true"|"false">`	Enable D leases ca custom `pihole-s`
`DHCP_START`	unset	`<Start IP>`	Start of t to hand (mandat enabled)
`DHCP_END`	unset	`<End IP>`	End of th to hand (mandat enabled)
`DHCP_ROUTER`	unset	`<Router's IP>`	Router (g by the D DHCP se

Variable	Default	Value	
`DHCP_LEASETIME`	24	`<hours>`	DHCP lea
`PIHOLE_DOMAIN`	`lan`	`<domain>`	Domain server.
`DHCP_IPv6`	`false`	`<"true"|"false">`	Enable D (SLAAC +
`DHCP_rapid_commit`	`false`	`<"true"|"false">`	Enable D (fast add
`VIRTUAL_HOST`	`${HOSTNAME}`	`<Custom Hostname>`	What yo host' is, this Host make ch blacklist default ' address
`IPv6`	`true`	`<"true"|"false">`	For unra out all th from DN false.
`TEMPERATUREUNIT`	`c`	`<c|k|f>`	Set prefe `c` : Celsi Fahrenh
`WEBUIBOXEDLAYOUT`	`boxed`	`<boxed|traditional>`	Use boxe working
`QUERY_LOGGING`	`true`	`<"true"|"false">`	Enable q

Variable	Default	Value	
`WEBTHEME`	`default-light`	`<"default-dark"|"default-darker"|"default-light"|"default-auto"|"high-contrast"|"high-contrast-dark"|"lcars">`	User inte
`WEBPASSWORD_FILE`	unset	`<Docker secret path>`	Set an A Docker s set, `WEB` If `WEBPA` `WEBPASS` valid rea `WEBPASS` contents

Advanced Variables

Variable	Default	Value	De
`INTERFACE`	unset	`<NIC>`	The default works f example docker ru trying to use DHCP then you may have DNSMASQ_LISTENI

Variable	Default	Value	De
`DNSMASQ_LISTENING`	unset	`<local|all|single>`	`local` listens on al permits listening or in addition to local, the interface specifi
`WEB_PORT`	unset	`<PORT>`	**This will break the functionality of Pi-** advanced setups lik or `--net=host` doc explains how to res functionality using a [Alternative Synolog]
`WEB_BIND_ADDR`	unset	`<IP>`	Lighttpd's bind add will bind to every in running in host net will use `FTLCONF_LO`
`SKIPGRAVITYONBOOT`	unset	`<unset|1>`	Use this option to s Database when boo default this environ the Gravity Databas the container starts environment variab cause the Gravity D when container star
`CORS_HOSTS`	unset	`<FQDNs delimited by ,>`	List of domains/sub is allowed. Wildcard

Variable	Default	Value	De

			`CORS_HOSTS:`
			`domain.com,home.do`

`CUSTOM_CACHE_SIZE`	`10000`	Number	Set the cache size f increasing the defa 0. Note that when setting is ignored.
`FTL_CMD`	`no-daemon`	`no-daemon -- <dnsmasq option>`	Customize the optic gets started. e.g. `n` `forward-max 300` to concurrent dns que
`FTLCONF_[SETTING]`	unset	As per documentation	Customize pihole-F described in the FTI For example, to cus ensure you have th environment variab

Experimental Variables

Variable	Default	Value	Description
`DNSMASQ_USER`	unset	`<pihole|root>`	Allows changing the user that FTLDNS runs as. Default: `pihole` , some systems such as Synology NAS may require you to

Variable	Default	Value	Description
			change this to `root` (See [#963](#963))
`PIHOLE_UID`	`999`	Number	Overrides image's default pihole user id to match a host user id **IMPORTANT**: id must not already be in use inside the container!
`PIHOLE_GID`	`999`	Number	Overrides image's default pihole group id to match a host group id **IMPORTANT**: id must not already be in use inside the container!
`WEB_UID`	`33`	Number	Overrides image's default www-data user id to match a host user id **IMPORTANT**: id must not already be in use inside the container! (Make sure it is different to `PIHOLE_UID` if you are using that, also)
`WEB_GID`	`33`	Number	Overrides image's default www-data group id to match a host group id **IMPORTANT**: id must not

Variable	Default	Value	Description
			already be in use inside the container! (Make sure it is different to `PIHOLE_GID` if you are using that, also)
`WEBLOGS_STDOUT`	0	0|1	0 logs to defined files, 1 redirect access and error logs to stdout

Deprecated environment variables:

While these may still work, they are likely to be removed in a future version. Where applicable, alternative variable names are indicated. Please review the table above for usage of the alternative variables

Docker Environment Var.	Description	Replaced By
`CONDITIONAL_FORWARDING`	Enable DNS conditional forwarding for device name resolution	`REV_SERVER`
`CONDITIONAL_FORWARDING_IP`	If conditional forwarding is enabled, set the IP of the local network router	`REV_SERVER_TARGET`

Docker Environment Var.	Description	Replaced By
`CONDITIONAL_FORWARDING_DOMAIN`	If conditional forwarding is enabled, set the domain of the local network router	`REV_SERVER_DOMAIN`
`CONDITIONAL_FORWARDING_REVERSE`	If conditional forwarding is enabled, set the reverse DNS of the local network router (e.g. `0.168.192.in-addr.arpa`)	`REV_SERVER_CIDR`
`DNS1`	Primary upstream DNS provider, default is google DNS	`PIHOLE_DNS_`
`DNS2`	Secondary upstream DNS provider, default is google DNS, `no` if only one	`PIHOLE_DNS_`

Docker Environment Var.	Description	Replaced By
	DNS should used	
`ServerIP`	Set to your server's LAN IP, used by web block modes and lighttpd bind address	`FTLCONF_LOCAL_IPV4`
`ServerIPv6`	**If you have a v6 network** set to your server's LAN IPv6 to block IPv6 ads fully	`FTLCONF_LOCAL_IPV6`
`FTLCONF_REPLY_ADDR4`	Set to your server's LAN IP, used by web block modes and lighttpd bind address	`FTLCONF_LOCAL_IPV4`
`FTLCONF_REPLY_ADDR6`	**If you have a v6 network** set to your server's LAN	`FTLCONF_LOCAL_IPV6`

Docker Environment Var.	Description	Replaced By
	IPv6 to block IPv6 ads fully	

To use these env vars in docker run format style them like: `-e DNS1=1.1.1.1`

Here is a rundown of other arguments for your docker-compose / docker run.

Docker Arguments	Description
`-p <port>:<port>` **Recommended**	Ports to expose (53, 80, 67), the bare minimum ports required for Pi-holes HTTP and DNS services
`--restart=unless-stopped` **Recommended**	Automatically (re)start your Pi-hole on boot or in the event of a crash
`-v $(pwd)/etc-pihole:/etc/pihole` **Recommended**	Volumes for your Pi-hole configs help persist changes across docker image updates
`-v $(pwd)/etc-dnsmasq.d:/etc/dnsmasq.d` **Recommended**	Volumes for your dnsmasq configs help persist changes across docker image updates
`--net=host` *Optional*	Alternative to `-p <port>:<port>` arguments (Cannot be used at same time as -p) if you don't run any other web application. DHCP runs best with --net=host, otherwise your router must support dhcp-relay settings.

Docker Arguments	Description
`--cap-add=NET_ADMIN` *Recommended*	Commonly added capability for DHCP, see [Note on Capabilities](#) below for other capabilities.
`--dns=127.0.0.1` *Optional*	Sets your container's resolve settings to localhost so it can resolve DHCP hostnames from Pi-hole's DNSMasq, may fix resolution errors on container restart.
`--dns=1.1.1.1` *Optional*	Sets a backup server of your choosing in case DNSMasq has problems starting
`--env-file .env` *Optional*	File to store environment variables for docker replacing `-e key=value` settings. Here for convenience

Tips and Tricks

- A good way to test things are working right is by loading this page: http://pi.hole/admin/
- How do I set or reset the Web interface Password?
  - `docker exec -it pihole_container_name pihole -a -p` - then enter your password into the prompt
- Port conflicts? Stop your server's existing DNS / Web services.
  - Don't forget to stop your services from auto-starting again after you reboot
  - Ubuntu users see below for more detailed information
- You can map other ports to Pi-hole port 80 using docker's port forwarding like this `-p 8080:80` if you are using the default blocking mode. If you are

using the legacy IP blocking mode, you should not remap this port.
    - Here is an example of running with nginxproxy/nginx-proxy (an nginx auto-configuring docker reverse proxy for docker) on my port 80 with Pi-hole on another port. Pi-hole needs to be `DEFAULT_HOST` env in nginxproxy/nginx-proxy and you need to set the matching `VIRTUAL_HOST` for the Pi-hole's container. Please read nginxproxy/nginx-proxy readme for more info if you have trouble.
- Docker's default network mode `bridge` isolates the container from the host's network. This is a more secure setting, but requires setting the Pi-hole DNS option for *Interface listening behavior* to "Listen on all interfaces, permit all origins".

Installing on Ubuntu or Fedora

Modern releases of Ubuntu (17.10+) and Fedora (33+) include `systemd-resolved` which is configured by default to implement a caching DNS stub resolver. This will prevent pi-hole from listening on port 53. The stub resolver should be disabled with: `sudo sed -r -i.orig 's/#?DNSStubListener=yes/DNSStubListener=no/g' /etc/systemd/resolved.conf`

This will not change the nameserver settings, which point to the stub resolver thus preventing DNS resolution. Change the `/etc/resolv.conf` symlink to point to `/run/systemd/resolve/resolv.conf`, which is automatically updated to follow the system's `netplan`: `sudo sh -c 'rm /etc/resolv.conf && ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf'` After making these changes, you should restart systemd-resolved using `systemctl restart systemd-resolved`

Once pi-hole is installed, you'll want to configure your clients to use it (see here). If you used the symlink above, your docker host will either use whatever is served by DHCP, or whatever static setting you've configured. If you want to explicitly set your docker host's nameservers you can edit the netplan(s) found at `/etc/netplan`, then run `sudo netplan apply`. Example netplan:

```
network:
    ethernets:
        ens160:
            dhcp4: true
            dhcp4-overrides:
                use-dns: false
            nameservers:
                addresses: [127.0.0.1]
    version: 2
```

Note that it is also possible to disable `systemd-resolved` entirely. However, this can cause problems with name resolution in vpns (see bug report). It also disables the functionality of netplan since systemd-resolved is used as the default renderer (see `man netplan`). If you choose to disable the service, you will need to manually set the nameservers, for example by creating a new `/etc/resolv.conf`.

Users of older Ubuntu releases (circa 17.04) will need to disable dnsmasq.

Installing on Dokku

@Rikj000 has produced a guide to assist users installing Pi-hole on Dokku

Docker tags and versioning

The primary docker tags are explained in the following table. Click here to see the full list of tags. See GitHub Release notes to see the specific version of Pi-hole Core, Web, and FTL included in the release.

The Date-based (including incremented "Patch" versions) do not relate to any kind of semantic version number, rather a date is used to differentiate between the new version and the old version, nothing more. Release notes will always contain full details of changes in the container, including changes to core Pi-hole components

tag	description
`latest`	Always latest release
`2022.04.0`	Date-based release
`2022.04.1`	Second release in a given month
`dev`	Similar to `latest`, but for the development branch (pushed occasionally)
`*beta`	Early beta releases of upcoming versions - here be dragons
`nightly`	Like `dev` but pushed every night and pulls from the latest `development` branches of the core Pi-hole components (Pi-hole, web, FTL)

Upgrading, Persistence, and Customizations

The standard Pi-hole customization abilities apply to this docker, but with docker twists such as using docker volume mounts to map host stored file configurations over the container defaults. However, mounting these configuration files as read-only should be avoided. Volumes are also important to persist the configuration in case you have removed the Pi-hole container which is a typical docker upgrade pattern.

Upgrading / Reconfiguring

Do not attempt to upgrade (`pihole -up`) or reconfigure (`pihole -r`). New images will be released for upgrades, upgrading by replacing your old container with a fresh upgraded image is the 'docker way'. Long-living docker containers are not the docker way since they aim to be portable and reproducible, why not re-create them often! Just to prove you can.

0. Read the release notes for both this Docker release and the Pi-hole release
    - This will help you avoid common problems due to any known issues with upgrading or newly required arguments or variables
    - We will try to put common break/fixes at the top of this readme too
1. Download the latest version of the image: `docker pull pihole/pihole`
2. Throw away your container: `docker rm -f pihole`
    - **Warning** When removing your pihole container you may be stuck without DNS until step 3; **docker pull** before **docker rm -f** to avoid DNS interruption **OR** always have a fallback DNS server configured in DHCP to avoid this problem altogether.
    - If you care about your data (logs/customizations), make sure you have it volume-mapped or it will be deleted in this step.

3. Start your container with the newer base image: `docker run <args> pihole/pihole` (`<args>` being your preferred run volumes and env vars)

Why is this style of upgrading good? A couple reasons: Everyone is starting from the same base image which has been tested to known it works. No worrying about upgrading from A to B, B to C, or A to C is required when rolling out updates, it reduces complexity, and simply allows a 'fresh start' every time while preserving customizations with volumes. Basically I'm encouraging phoenix server principles for your containers.

To reconfigure Pi-hole you'll either need to use an existing container environment variables or if there is no a variable for what you need, use the web UI or CLI commands.

Pi-hole features

Here are some relevant wiki pages from Pi-hole's documentation. The web interface or command line tools can be used to implement changes to pihole.

We install all pihole utilities so the the built in pihole commands will work via `docker exec <container> <command>` like so:

- `docker exec pihole_container_name pihole updateGravity`
- `docker exec pihole_container_name pihole -w spclient.wg.spotify.com`
- `docker exec pihole_container_name pihole -wild example.com`

Customizations

The webserver and DNS service inside the container can be customized if necessary. Any configuration files you volume mount into `/etc/dnsmasq.d/` will be loaded by dnsmasq when the container starts or restarts or if you need to modify the Pi-hole config it is located at `/etc/dnsmasq.d/01-pihole.conf`. The docker start scripts runs a config test prior to starting so it will tell you about any errors in the docker log.

Similarly for the webserver you can customize configs in /etc/lighttpd

Systemd init script

As long as your docker system service auto starts on boot and you run your container with `--restart=unless-stopped` your container should always start on boot and restart on crashes. If you prefer to have your docker container run as a systemd service instead, add the file pihole.service to "/etc/systemd/system"; customize whatever your container name is and remove `--restart=unless-stopped` from your docker run. Then after you have initially created the docker container using the docker run command above, you can control it with "systemctl start pihole" or "systemctl stop pihole" (instead of `docker start` / `docker stop`). You can also enable it to auto-start on boot with "systemctl enable pihole" (as opposed to `--restart=unless-stopped` and making sure docker service auto-starts on boot).

NOTE: After initial run you may need to manually stop the docker container with "docker stop pihole" before the systemctl can start controlling the container.

Note on Capabilities

DNSMasq / FTLDNS expects to have the following capabilities available:

- `CAP_NET_BIND_SERVICE` : Allows FTLDNS binding to TCP/UDP sockets below 1024 (specifically DNS service on port 53)
- `CAP_NET_RAW` : use raw and packet sockets (needed for handling DHCPv6 requests, and verifying that an IP is not in use before leasing it)
- `CAP_NET_ADMIN` : modify routing tables and other network-related operations (in particular inserting an entry in the neighbor table to answer DHCP requests using unicast packets)
- `CAP_SYS_NICE` : FTL sets itself as an important process to get some more processing time if the latter is running low
- `CAP_CHOWN` : we need to be able to change ownership of log files and databases in case FTL is started as a different user than `pihole`

This image automatically grants those capabilities, if available, to the FTLDNS process, even when run as non-root.
By default, docker does not include the `NET_ADMIN` capability for non-privileged containers, and it is recommended to explicitly add it to the container using `--cap-add=NET_ADMIN` .
However, if DHCP and IPv6 Router Advertisements are not in use, it should be safe to skip it. For the most paranoid, it should even be possible to explicitly drop the `NET_RAW` capability to prevent FTLDNS from automatically gaining it.

Note on Watchtower

We have noticed that a lot of people use Watchtower to keep their Pi-hole containers up to date. For the same reason we don't provide an auto-update feature on a bare metal install, you *should not* have a system automatically update your Pi-hole container. Especially unattended. As much as we try to ensure nothing will go wrong, sometimes things do go wrong - and you need to set aside time to *manually* pull and update to the version of the container you wish to run. The upgrade process should be along the lines of:

- **Important**: Read the release notes. Sometimes you will need to make changes other than just updating the image
- Pull the new image
- Stop and *remove* the running Pi-hole container
  - If you care about your data (logs/customizations), make sure you have it volume-mapped or it will be deleted in this step.
- Recreate the container using the new image

Pi-hole is an integral part of your network, don't let it fall over because of an unattended update in the middle of the night.

User Feedback

Please report issues on the GitHub project when you suspect something docker related. Pi-hole or general docker questions are best answered on our user forums.

pi-hole / pi-hole Public

<> **Code** Issues 32 Pull requests 18 Discussions Actions Projects 1 Security 1 Insights

master ▾ Go to file Code

PromoFaux v5.17.2 (#5421) ... ✓ on Oct 11 **5,818**

.github	Bump actions/setup-python from 4.7.0 to 4.7.1	last month
advanced	adminlte->web	last month
automated install	adminlte->web	last month
manpages	adminlte->web	last month
test	Yu vs uh	last month
.codespellignore	Adds spellcheck action to the smoke-tests (als...	last year
.editorconfig	Add editorconfig-checker workflow	last year
.gitattributes	linux style line endings enforced	6 years ago
.gitignore	Update the tests (#4427)	2 years ago
.stickler.yml	Disable line length rule for yamllint - fix indent...	last year
.yamllint.conf	Disable line length rule for yamllint - fix indent...	last year
CONTRIBUTING.md	Add editorconfig-checker workflow	last year
LICENSE	[Staging] 3.1 (#1502)	6 years ago

About

A black hole for Internet advertisements

pi-hole.net

#shell #raspberry-pi #cloud #dashboard #dhcp #pi-hole #ad-blocker #dnsmasq #dhcp-server #blocker #dns-server

Readme

View license

Code of conduct

Security policy

Activity

45.2k stars

702 watching

2.6k forks

Report repository

Releases 101

v5.17.2 Latest
on Oct 11

README.md	adminlte->web	last month
gravity.sh	Remove user agent when downloading adlists	2 months ago
pihole	Only source versions file if the file exits	10 months ago

---

Network-wide ad blocking via your own Linux hardware

The Pi-hole® is a DNS sinkhole that protects your devices from unwanted content without installing any client-side software.

- **Easy-to-install**: our dialogs walk you through the simple installation process in less than ten minutes
- **Resolute**: content is blocked in *non-browser locations*, such as ad-laden mobile apps and smart TVs

+ 100 releases

Sponsor this project

pi-hole Pi-hole

https://pi-hole.net/donate

patreon.com/**pihole**

Learn more about GitHub Sponsors

Packages

No packages published

Contributors 220

+ 206 contributors

Languages

- **Responsive**: seamlessly speeds up the feel of everyday browsing by caching DNS queries
- **Lightweight**: runs smoothly with minimal hardware and software requirements
- **Robust**: a command-line interface that is quality assured for interoperability
- **Insightful**: a beautiful responsive Web Interface dashboard to view and control your Pi-hole

README.md

devices are protected automatically

- **Scalable**: capable of handling hundreds of millions of queries when installed on server-grade hardware
- **Modern**: blocks ads over both IPv4 and IPv6
- **Free**: open source software that helps ensure *you* are the sole person in control of your privacy

● **Shell** 83.7% ● **Python** 12.3%
● **Roff** 2.5% ● **Dockerfile** 1.5%

One-Step Automated Install

Those who want to get started quickly and conveniently may install Pi-hole using the following command:

```
curl -sSL https://install.pi-hole.net | bash
```

Alternative Install Methods

Piping to `bash` is controversial, as it prevents you from reading code that is about to run on your system. Therefore, we provide these alternative installation methods which allow code review before installation:

Method 1: Clone our repository and run

```
git clone --depth 1 https://github.com/pi-hole/pi-hole.git Pi-hole
cd "Pi-hole/automated install/"
sudo bash basic-install.sh
```

Method 2: Manually download the installer and run

```
wget -O basic-install.sh https://install.pi-hole.net
sudo bash basic-install.sh
```

Method 3: Using Docker to deploy Pi-hole

Please refer to the Pi-hole docker repo to use the Official Docker Images.

Post-install: Make your network take advantage of Pi-hole

Once the installer has been run, you will need to configure your router to have **DHCP clients use Pi-hole as their DNS server**. This router configuration will ensure that all devices connecting to your network will have content blocked without any further intervention.

If your router does not support setting the DNS server, you can use Pi-hole's built-in DHCP server; be sure to disable DHCP on your router first (if it has that feature available).

As a last resort, you can manually set each device to use Pi-hole as their DNS server.

Pi-hole is free but powered by your support

There are many reoccurring costs involved with maintaining free, open-source, and privacy-respecting software; expenses which our volunteer developers pitch in to cover out-of-pocket. This is just one example of how strongly we feel about our software and the importance of keeping it maintained.

Make no mistake: **your support is absolutely vital to help keep us innovating!**

Donations

Donating using our Sponsor Button is **extremely helpful** in offsetting a portion of our monthly expenses:

Alternative support

If you'd rather not donate (*which is okay!*), there are other ways you can help support us:

- GitHub Sponsors
- Patreon
- Hetzner Cloud *affiliate link*
- Digital Ocean *affiliate link*
- Stickermule *earn a $10 credit after your first purchase*
- Amazon US *affiliate link*
- Spreading the word about our software and how you have benefited from it

Contributing via GitHub

We welcome *everyone* to contribute to issue reports, suggest new features, and create pull requests.

If you have something to add - anything from a typo through to a whole new feature, we're happy to check it out! Just make sure to fill out our template when submitting your request; the questions it asks will help the volunteers quickly understand what you're aiming to achieve.

You'll find that the install script and the debug script have an abundance of comments, which will help you better understand how Pi-hole works. They're also a valuable resource to those who want to learn how to write scripts or code a program! We encourage anyone who likes to tinker to read through it and submit a pull request for us to review.

Getting in touch with us

While we are primarily reachable on our Discourse User Forum, we can also be found on various social media outlets.

Please be sure to check the FAQs before starting a new discussion, as we do not have the spare time to reply to every request for assistance.

- Frequently Asked Questions
- Feature Requests
- Reddit
- Twitter

Breakdown of Features

Faster-than-light Engine

FTLDNS is a lightweight, purpose-built daemon used to provide statistics needed for the Web Interface, and its API can be easily integrated into your own projects. As the name implies, FTLDNS does this all *very quickly*!

Some of the statistics you can integrate include:

- Total number of domains being blocked
- Total number of DNS queries today
- Total number of ads blocked today
- Percentage of ads blocked
- Unique domains
- Queries forwarded (to your chosen upstream DNS server)
- Queries cached
- Unique clients

Access the API via `telnet`, the Web (`admin/api.php`) and Command Line (`pihole -c -j`). You can find out more details over here.

The Command-Line Interface

The pihole command has all the functionality necessary to fully administer the Pi-hole, without the need for the Web Interface. It's fast, user-friendly, and auditable by anyone with an understanding of `bash`.

Some notable features include:

- Whitelisting, Blacklisting, and Regex
- Debugging utility
- Viewing the live log file
- Updating Ad Lists
- Querying Ad Lists for blocked domains

- Enabling and Disabling Pi-hole
- ... and *many* more!

You can read our Core Feature Breakdown for more information.

The Web Interface Dashboard

This optional dashboard allows you to view stats, change settings, and configure your Pi-hole. It's the power of the Command Line Interface, with none of the learning curve!

Some notable features include:

- Mobile-friendly interface
- Password protection
- Detailed graphs and doughnut charts
- Top lists of domains and clients
- A filterable and sortable query log
- Long Term Statistics to view data over user-defined time ranges
- The ability to easily manage and configure Pi-hole features
- ... and all the main features of the Command Line Interface!

There are several ways to access the dashboard:

1. `http://pi.hole/admin/` (when using Pi-hole as your DNS server)
2. `http://<IP_ADDRESS_OF_YOUR_PI_HOLE>/admin/`

raspberrytips.com

How to Install Pi-Hole on Ubuntu (Beginner's Guide)

Patrick Fromaget

10–13 minutes

Ads are all over the place on the Internet. Most people develop a sixth sense to ignore them, use a browser extension like AdBlock to hide some of them, or block everything on their whole network by installing Pi-Hole on Ubuntu. How do you do this? I will explain my setup in this article.

Pi-Hole is a free and open-source ad blocker that can be installed on any Linux distribution with only one command line: “curl -sSL https://install.pi-hole.net | bash”. Once done, the network configuration needs to be updated to use it as the main DNS server.

This might seem simple at first glance, but I bet you’ll need more details on how to do this safely and efficiently. Keep reading to see how to set up Pi-Hole step-by-step on your network.

If you’re looking to quickly progress on Raspberry Pi, you can check out my e-book here. It’s a 30-day challenge where you learn one new thing every day until you become a Raspberry Pi expert. The first third of the book teaches you the basics, but the following chapters include projects you can try on your own.

Linux doesn’t have to be intimidating. With my e-book, **Master Linux Commands**, you’ll uncover the secrets of the terminal in a fun, step-by-step journey. From basics to scripts, get ready to level up your Linux skills. Oh, and did I mention the handy cheat sheet you get as a bonus?

Pi-Hole server Installation on Ubuntu

Pi-Hole requirements

Pi-Hole is a lightweight solution, and that doesn't require much processing power to install it. In fact, it's mainly used on the Raspberry Pi, a tiny computer with limited CPU and RAM, so it shouldn't be an issue on any standard computer.

In their documentation, **Pi-Hole recommends at least 2 GB of free space on the disk and 512 MB RAM.**

Your computer will be perfect, but you can also use a Raspberry Pi 4 or a minimal Intel NUC for example. I read that you can even install it on a Synology NAS, with a docker container (I have this one on Amazon, but you can find cheaper models).

Warning: Pi-Hole may not be supported on the latest Ubuntu release, check this link to verify.

You can install Pi-Hole directly on your computer if you are using Ubuntu, but it's probably better to install it on something you'll run 24/7. For example, if you configure the whole network to use Pi-Hole, Internet won't work on other devices if your computer is off or in sleeping mode. This would not be a great experience.

That's why I suggest using a Raspberry Pi (you can install Ubuntu on it), a NAS or any device that you can leave running all the time.

Linux commands to elevate your skills!
Download now

Note: If you are trying this on a Raspberry Pi with the default operating system, I have a detailed tutorial on how to install Pi-Hole on Raspberry Pi. In this article, I’ll focus on Ubuntu.

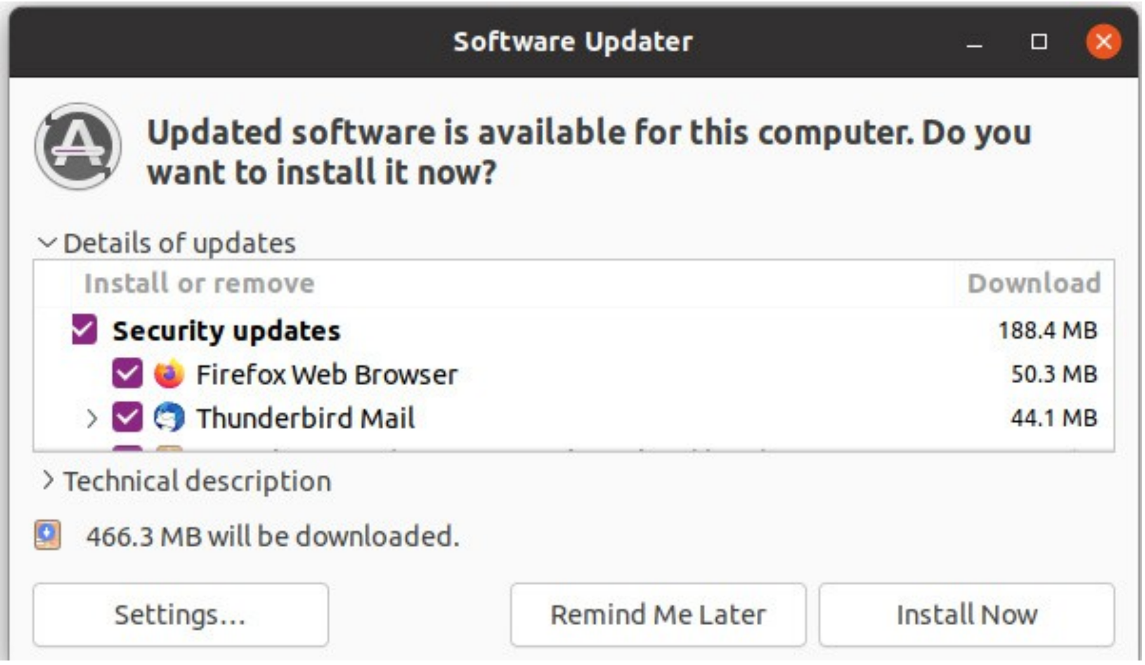
Update your operating system

Once your hardware is selected and Ubuntu is installed, the first thing to do is to update your system. It’s a good practice to follow before installing anything on your system, just to avoid dependency issues and version incompatibility.

You can do this easily in a terminal:

```
sudo apt update
sudo apt upgrade
```

Or use the software updater tool in the graphic interface if you are using the Desktop version:



Updated software is available for this computer. Do you want to install it now?

Install or remove	Download
☑ **Security updates**	188.4 MB
☑ Firefox Web Browser	50.3 MB
☑ Thunderbird Mail	44.1 MB

466.3 MB will be downloaded.

Click on “Install now” and type the user password to confirm the installation.
A reboot is probably a good idea if you have many updates to

catch up on.

Then you'll also need to install curl on your system if not already there:

```
sudo apt install curl
```

The Pi-Hole script will install anything else after that.

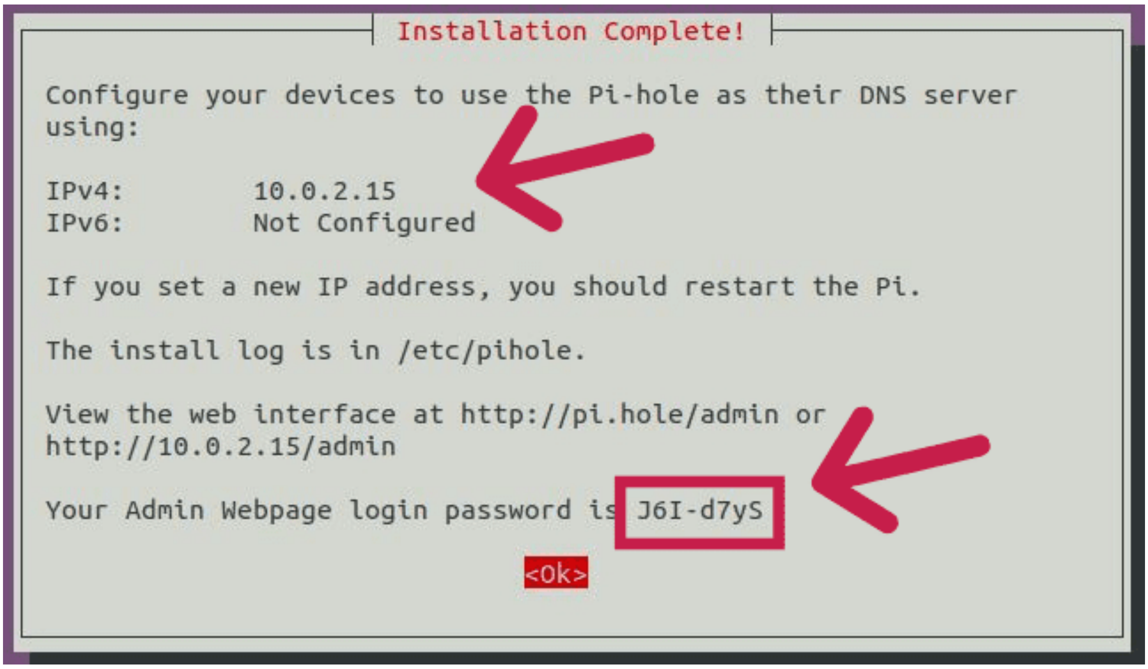
Pi-Hole installation script

Once your system is ready, the installation can be done with only one command, by copying and pasting this into a terminal:

```
curl -sSL https://install.pi-hole.net | bash
```

The process is almost automatic, but you still need to answer a few questions to adjust your settings:

Make sure to not use the default password and move to the next step.



```
Installation Complete!

Configure your devices to use the Pi-hole as their DNS server
using:

IPv4:        10.0.2.15
IPv6:        Not Configured

If you set a new IP address, you should restart the Pi.

The install log is in /etc/pihole.

View the web interface at http://pi.hole/admin or
http://10.0.2.15/admin

Your Admin Webpage login password is J6I-d7yS

<Ok>
```

Configure your clients to use Pi-Hole

Once your server is installed, the next step is to configure your network to use this server. Pi-Hole works like a DNS server, so you need to change the primary DNS server on all of the devices to use the Pi-Hole IP address.

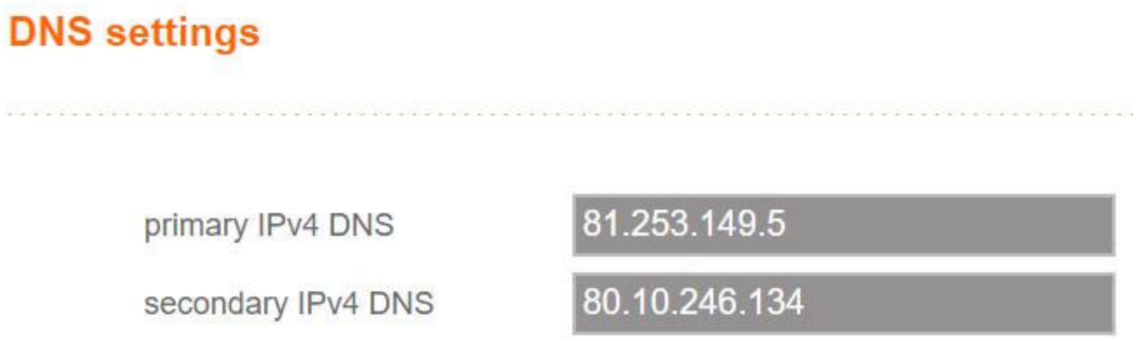
This can be done manually on each device, but the easiest way is to change the default DNS server in your DHCP configuration.

Edit the DHCP configuration to set Pi-Hole as the default DNS

The easiest way to config all devices at once is to go to your DHCP server configuration and set the primary DNS server to the Pi-Hole server IP address.

If you are installing this at home, your DHCP server is probably your Internet router.
I won't explain how to do this in detail, as it will be different for each provider and router, but as a whole, the idea is to find the DHCP settings on the web interface and change the DNS server IP address.

By default, it's probably the DNS server from your provider.
In my case, it was in the DNS settings:



DNS settings

primary IPv4 DNS 81.253.149.5
secondary IPv4 DNS 80.10.246.134

Once you find something like this, remove the default values and set the primary DNS server to your Pi-Hole installation IP address (probably something like 192.168.1.X or 192.168.0.X). Leave the secondary DNS server empty.

It may take a few hours to update the configuration on all devices on your network, but it will be done automatically.

Change the network configuration on each client to use Pi-Hole

The alternative is to manually update the configuration on each device you want to use with Pi-Hole. This might take more time, especially if you have many devices on your network, but this way you can make sure everything is working before breaking the Internet for the whole family!

On Windows 10:

- Right-click on the "Start Menu" and choose "Network Connections".
- Then click on "Change adapter settings".
- Right-click on your current connection and choose "Properties".
- Double-click on "Internet Protocol Version 4 (TCP/IPv4)".
- Set the DNS server to static and enter your Pi-Hole server IP Address.
  Keep the secondary DNS server empty.

On Linux and Mac OS:

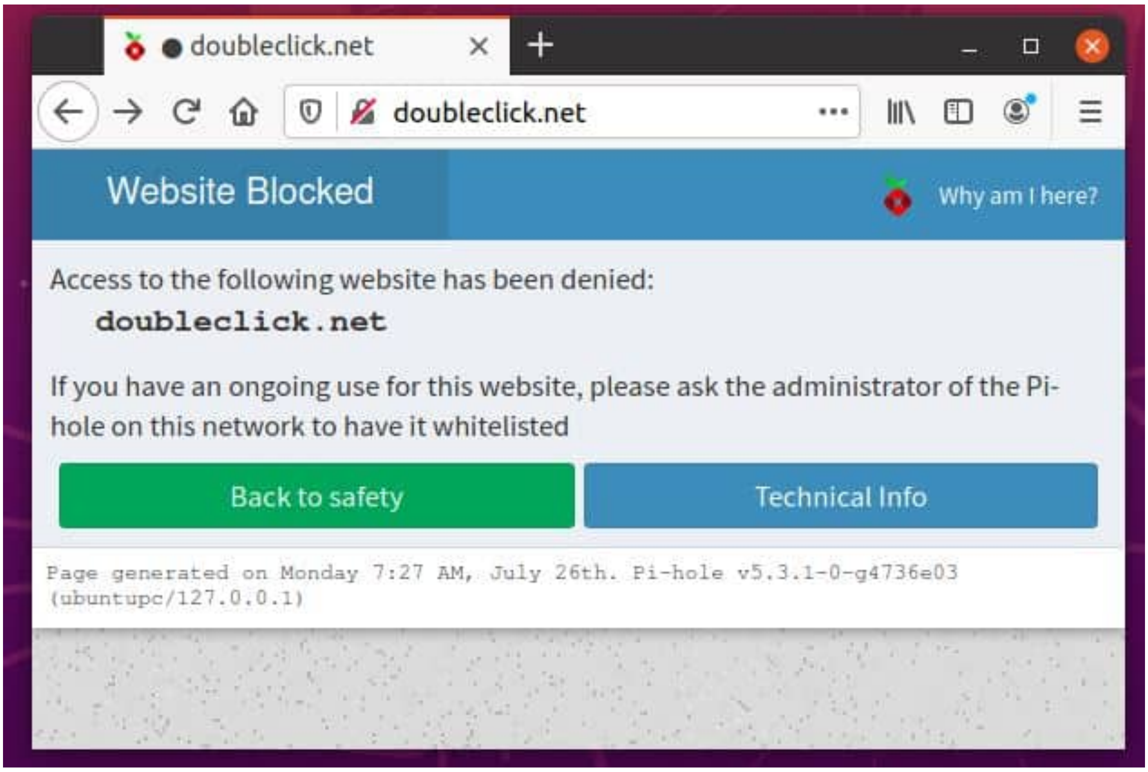
- If you have a graphical interface, you'll find the network settings in the System Preferences.
- If not, you can edit the /etc/resolv.conf file and replace the current DNS server with the Pi-Hole IP address.
  I explain how to change the DNS server on a server edition of

Linux in more details in this article. Click on the link to learn more, as the resolv.conf file might not work depending on your distribution.

On mobile, it's in your Wi-Fi settings.
Click details or edit the network on a network to see the DNS configuration.

How to know if Pi-Hole is working?

To know if Pi-Hole is working, you can go to the web interface and check if it's blocking ads. Another way is to try to access a domain hosting ad (like doubleclick.net) and verify that the Pi-Hole page appears instead of the website content.



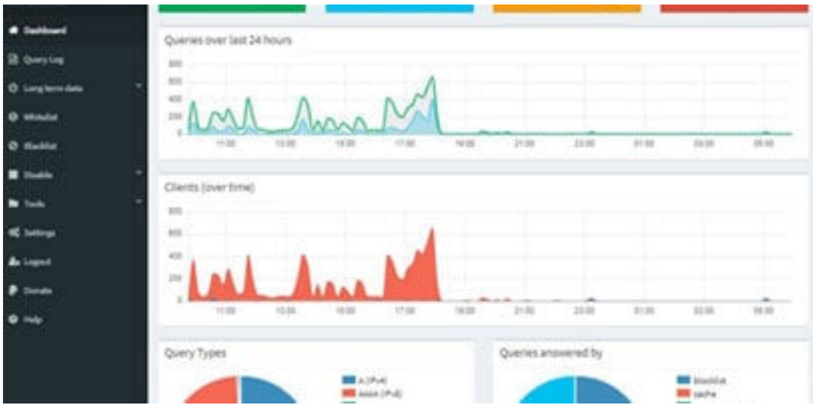
Access to the following website has been denied:

doubleclick.net

If you have an ongoing use for this website, please ask the administrator of the Pi-hole on this network to have it whitelisted

```
Page generated on Monday 7:27 AM, July 26th. Pi-hole v5.3.1-0-g4736e03
(ubuntupc/127.0.0.1)
```

The web interface is enabled on http://localhost/admin (if installed on your computer) or http://IP_Address/admin (if installed on another computer). The default password is provided at the end of the installation.



Pi-Hole FAQ

Can Pi-Hole run on any Linux distribution?

Pi-Hole is officially supported on Raspberry Pi OS (Raspbian), Ubuntu, Debian, Fedora and CentOS. As most Linux distributions are based on them, they should run on almost any of them.

Just check the exact supported release on this page before trying to install it. They are often a little behind when a new version is available. For example, at the time of writing (July 2021, Ubuntu 21.04 is not yet supported).

Consider using docker if you experience any compatibility issues with your system.

What can Pi-Hole be installed on?

The prerequisites to install Pi-Hole are 2 GB of disk space and 512 MB of RAM, so it can run on almost any computer, even the older ones. Raspberry Pi and other single-board computers are also supported as long as a supported operating system is installed.

My recommendation is to use a Raspberry Pi (as it's the cheapest option), plug it somewhere on your network and keep it on all the time.

Warning: current prices are all over the place for a new Raspberry Pi. Make sure to check this article to pay the right price when buying a Raspberry Pi. I also give a few tips to find one in stock (which currently isn't that easy).

What can I do with Pi-Hole?

The main purpose of Pi-Hole is to block ads on the Internet, by blocking their servers at a network level. Pi-Hole can also be used as a DHCP server and a network monitor.

Does Pi-Hole stop YouTube ads?

As Pi-Hole is working at a network level, it's not the best option to block YouTube ads. On YouTube, ads and videos are served from the same domain, so Pi-Hole will block both or none, it can't analyze the exact content.

If blocking YouTube ads is your main goal, a browser extension like AdBlock has a better chance of success.

Does Pi-Hole stop malware and phishing?

Pi-Hole won't natively stop malware and phishing on your devices, but you can add additional block lists with domains that are known to host malware or act as phishing. It won't have a 100% success rate, but it might increase the overall security of your network.

Your Go-To Linux Command Reference!

Download your exclusive free PDF containing the most useful Linux commands to elevate your skills!
Download now

Want to chat with other Raspberry Pi enthusiasts? Join the community, share your current projects and ask for help directly in the forums.

Additional Resources

Overwhelmed with Linux commands?
My e-book, "Master Linux Commands", is your essential guide to mastering the terminal. Get practical tips, real-world examples, and a bonus cheat sheet to keep by your side.
Grab your copy now.

VIP Community
If you just want to hang out with me and other Linux fans, you can also join the community. I share exclusive tutorials and behind-the-scenes content there. Premium members can also visit the website without ads.
More details here.

Need help building something with Python?
Python is a great language to get started with programming on any Linux computer.
Learn the essentials, step-by-step, without losing time understanding useless concepts.
Get the e-book now.

I'm the lead author and owner of RaspberryTips.com.

My goal is to help you with your Raspberry Pi problems using detailed guides and tutorials.
In real life, I'm a Linux system administrator with web developer experience.

Linux Commands Cheat Sheet

65 Linux Commands

From

RaspberryTips

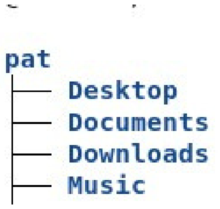
FILES MANAGEMENT

These commands are the basics that every Linux beginner should learn to browse the Linux files tree from a terminal

Reminder:

The Linux files organization is a tree, starting at /
Each subfolder adds a new level under /

For example, on the image you can see the tree for this folder : /home/pat



```
pat
├── Desktop
├── Documents
├── Downloads
└── Music
```

- ## CD <FOLDER>

Changes directory, go to the specified folder

Absolute path:	cd /home/pat/test
Relative path:	cd test

NB: "Absolute" is when you use the entire path
For "relative" you only enter the path from your current directory (in the second example, you need to already be in the /home/pat folder)

- ## MKDIR <FOLDER>

Creates a new subfolder in the current or specified path

Current directory:	mkdir test
Specific:	mkdir /home/pat/test

NB: The first example create a folder in your current directory (relative path)
The second one create a new directory in the exact parameter (absolute path)

- ## MV <SRC> <TARGET>

Moves a file or directory to another location (cut/paste)

Move a file:	mv test.txt /home/pat
Move a folder:	mv /home/pat/test /home/pat/test2

NB: The mv command is always in recursive mode

- ## MORE <FILENAME>

Displays the content of the file, page per page, from the beginning

Absolute path:	more test.txt
Relative path:	more /home/pat/test.txt

NB: For long files, you need to press "space" to continue, or "q" to quit

- ## LS (FOLDER)

Lists files and directory, in the current or specified folder

Current directory:	ls
Specific:	ls /home/pat/test

NB: You can use options with ls to get a more detailed view of files and folder, ex: ls -latr /home/pat

- ## CP <SOURCE> <TARGET>

Copies a file or directory to another location (copy/paste)

Copy a file	cp test.txt /home/pat
Recursive copy:	cp -r /home/pat/test /home/user/

NB: Use the recursive option to copy a folder and all its files and folders

- ## CAT <FILENAME>

Displays the content of the file, without pagination

Display on file:	cat test.txt
Use pattern:	cat *.txt

NB: A pattern allows you to display all files content for similar files

- ## TAIL <FILENAME>

Displays the end of the file

Basic usage:	tail test.txt
Lines count:	tail -n20 test.txt
Real-time display:	tail -f test.txt

NB: The -n option allows you to ask for a specific number of lines to display
The -f option refresh the display each time the file is modified (perfect for log files monitoring)

FILES MANAGEMENT (2)

- ## HEAD <FILENAME>

Similar to tail but to display the beginning of the file

Display 10 lines:	head test.xt
With lines count:	head -n20 test.txt

- ## TOUCH <FILENAME>

Create a new empty file

Current directory:	touch test.txt
Specific:	touch /home/pat/test.txt

NB: Most of the time, nano is a better choice to create a file, as you can edit it directly

- ## GREP

Grep is a powerful (and complex) tool to search string in a text or file

Find string in a file	grep "dhcp" /var/log/syslog
Filter a command output	ls -latr | grep ".php"
With a script:	/home/pat/script.sh | grep error

NB: The | option (pipe), allows you to run a command on another one output
You need to use quotes for complex search with space or special characters

There are also advanced usages possible:

Regular expressions:	grep "dhcp\\\|dns" /var/log/syslog
Command options:	grep -A2 -B4 'Fatal error' /var/log/syslog
Inverted search:	grep -v 'Notice' /var/log/syslogi

The | in the regular expressions allows you to use OR (one or more condition)
The -A option also catch X lines "after" the matched condition, -B is for "before"
Finally, the -v option is to filter lines that don't match the condition

- ## NANO <FILENAME>

Opens and edit the specified file. Nano is a powerful text editor in a terminal

Basic usage:	nano /home/pat/test.txt

NB: Nano will create the file if it doesn't exist

- ## RM <FILENAME>

Removes a file or directory

Remove file:	rm test.txt
Remove directory:	rm -rf /home/pat/test

NB: You need to use -rf options to remove a directory even if not empty (recursive + force)

- ## TAR

Tar is the linux way to manage compressed files

Create a new archive:	tar -cvfz archive.tar.gz /home/pat/test
Extract files	tar -xvfz archive.tar.gz

Options:
-c is to Compress, -x to eXtract
-v: verbose mode, -z: use gZip to compress, -f specify the file name
Use "man tar" for more information

- ## ZIP / UNZIP

Zip is similar to tar, but mainly used on Windows systems

Create a new archive:	zip -r archive.zip /home/pat/test
Extract files:	unzip archive.zip

NB: The -r option is to compress all the folder content
You can use the -d option to extract files in a specific folder
Use "man zip" or "man unzip" for all available options

FILES MANAGEMENT (3)

PWD

An easy command to display you current directory

Example:	pwd

FIND

Find allows you to search files on your computer, there are many options

Find a file name:	find /home/pat -iname test.txt
Filter extensions:	find /home/pat -iname *.php
Find only directories:	find / -type d -iname test

NB: -iname stands for "insensitive case", you can use -name if you prefer
You can use "-type f" to find only files

TREE

Another tool to get details on your current location, in a tree format

Current directory:	tree
Specific folder:	tree /home/pat/

NB: There are a few options to filter the output, by selecting only directory, managing symbolic links or setting a max depth level

More advanced options:

File size:	find / -size +10M
Recently modified files:	find /home -mtime -2

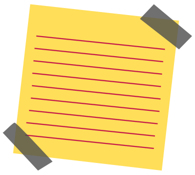
Run command on results:

find /var/log -iname *.log.gz -exec rm {} \;

The first command display all files over 10M on the disk
The -mtime -2 checks files modified in the last two days
The {} parameter in the last command will be replaced by the file name
Check the "man find" for more information

NETWORK COMMANDS

Here are the main commands to know to manage and use the network on your computer or server.



Reminder:

Most computers come with two interfaces or more : Ethernet and Wi-Fi.
In general, Ethernet is named eth0 and the Wi-Fi one is wlan0.

IFCONFIG / IP

Displays your current network configuration (IP Address, Mac Address, ...)

Usage: `ifconfig`

NB: Ifconfig is no longer included with all distributions.
Use "ip a" instead if it doesn't work.

IWCONFIG

Shows information about the wireless network configuration (SSID, speed, ...)

Usage: `iwconfig`

NB: You can also display a specific interface with iwconfig wlan0

IFUP / IFDOWN

Allows you to enable or disable one specific interface

Enable interface: `sudo ifup eth0`
Disable interface: `sudo ifdown eth0`

NB: It can help to disable the wireless interface while connected by cable

PING <HOST>

Checks if the host is alive

Basic usage: `ping 192.168.1.1`

NB: Read the "man ping" to see all available options

HOSTNAME

Displays or set the computer hostname

Display hostname: `hostname`
Set a new hostname: `sudo hostname MyLinuxServer`

WGET <URL>

Download a file with the terminal

Basic usage: `wget http://192.168.1.1/test.txt`
Change file name:
`wget http://192.168.1.1/test.txt -O target.txt`

SSH <USER>@<IP>

Connects to another Linux system with SSH

Example: `ssh pat@192.168.1.1`

SCP

Copies a file over the network by using SSH

Syntax: `scp <file> <user>@<ip>:<path>`
Example: `scp test.txt pat@192.168.1.1:/home/pat/`

RSYNC

Similar to SCP with more options like delta comparison and some other optimizations

Syntax: `rsync <file> <user>@<ip>:<path>`
Example: `rsync test.txt pat@192.168.1.1:/home/pat/`

Local copy: `rsync /home/pat/* /media/usb/`
Remote recursive copy: `rsync -auzr /home/pat/Documents/* pat@192.168.1.1:/home/pat/Documents/`

NB: Use "man rsync" to get all possible options

PACKAGES MANAGEMENT

Once you have the network working, you'll probably update your system and install the packages you need. On this page, you have all the required commands to do this from a terminal.

Vocabulary:

On Linux, each software is a **package**, as well as each **dependency.**
You are downloading new packages from **repositories** (servers hosting packages).
You need to use a tool called **apt** to search, install and updates packages on Debian-based OS.
All these commands need root privilege, you have to use sudo before each one.

APT UPDATE

Downloads the last packages list from your repositories

Usage:

```
sudo apt update
```

NB: To add a new repository, you can edit the apt configuration in /etc/apt/sources.list, or follow the instructions from the software editor

APT UPGRADE

Downloads and installs the latest version of each package available in the repository

Usage:

```
sudo apt upgrade
```

NB: You need to run apt update before doing this, to get the latest versions
The -y option allows you to automatically accept the installation

LIST INSTALLED PACKAGES

Dpkg can also be useful to list currently installed packages

Syntax:

```
dpkg -l
```

With grep:

```
dpkg -l | grep php
```

NB: Read the "man dpkg" output to get all possible options from this command

APT INSTALL <PACKAGE>

Installs the specified package on your system

Usage:

```
sudo apt install phpmyadmin
```

NB: Use the following search command to know the exact name of a package

APT REMOVE <PACKAGE>

Uninstall a package from your system

Usage:

```
sudo apt remove vim
```

APT SEARCH

Very useful to find the exact package name before installing it

Usage:

```
apt search openjdk
```

With grep:

```
apt search openjdk | grep jre
```

NB: You don't need sudo for this one

MANUAL INSTALLATION

Sometimes, you need to install packages manually, if the editor doesn't provide a repository

Download the file with wget:

```
wget https://www.realvnc.com/download/file/viewer.files/VNC-Viewer-6.19.325-Linux-amd64.deb
```

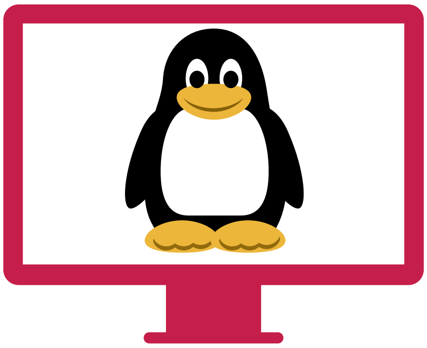
Manual installation:

```
sudo dpkg -i VNC-Viewer-6.19.325-Linux-amd64.deb
```

NB: You can use dpkg -r to remove a package manually, or dpkg-reconfigure to redo the configuration after installation

SYSTEM MANAGEMENT

Now that you have all packages installed, you may need to learn more advanced commands on how to manage your operating system.



REBOOT

This command will restart your computer immediately

Usage:	sudo reboot

SHUTDOWN

Stops the computer, now or at a specific time

Stop now:	sudo shutdown -h now
At a specific time:	sudo shutdown -h 20:00

SERVICE

Each daemon has an associated service, you can start or stop it when you want

Start:	sudo service apache2 start
Stop:	sudo service apache2 stop
Restart:	sudo service apache2 start
Reload config:	sudo service apache2 reload

NB: Use "service <service>" to list all available options, for example "service apache2"
The tab key will help you to find the service name

START SERVICE ON BOOT

Most of the time, services automatically start on boot, but if needed you can do this manually

Start on boot:	sudo update-rc.d ssh enable
Don't start on boot:	sudo update-rc.d -f ssh remove

NB: To start a script on boot, add it to the /etc/rc.local file

PROCESS LIST

Displays all running processes

Basic usage:	ps aux
Only by a specific user:	ps -u pat

NB: I give you the command to list currently installed packages in the next line

KILL / KILLALL

Immediately stop a specific process or all processes from the same command

Kill:	kill 12345
Killall:	killall php

NB: Use the ps command to find the process ID to kill

HTOP

A great alternative to top, to display system load and process in an intuitive interface

Usage:	htop

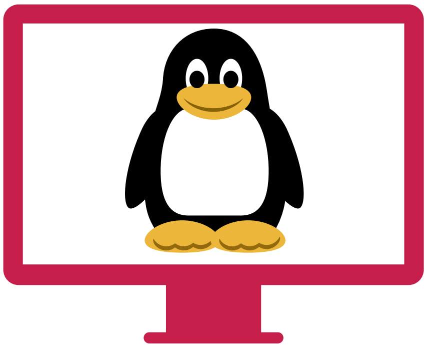
NB: htop is not installed by default, install it with "apt install htop"

DF

Displays your partition list, a good way to check the remaining disk space

Basic usage:	df
More readable:	df -h
Specific partition:	df -h /media/usb

SYSTEM MANAGEMENT (2)



DU

Displays the disk space usage in the current or specified folder

Basic usage:	du
Specific folder:	du /home/pat
Summarize:	du --summarize /home/pat
20 biggest files:	du -ak | sort -nr | head -20

NB: There are a lot more options, check the "man du" to find more help about this one

DATE

As the name says, display the current date and time

Full output:	date
Specific format:	date +%m-%d-%Y

NB: The "man date" command gives you the list of all availables options and format

CHOWN

Changes file owner and group

Change file owner:	sudo chown pat /usr/local/bin/script.sh
Change file owner & group:	sudo chown pat:www-data /var/www/html/mysite

MOUNT

Mount a new partition (usb key for example)

Mount disk:	sudo mount /dev/sda1 /mnt/usb
Unmount:	sudo umount /mnt/usb

NB: It's a complex command for beginner, but this post will give you all the needed informations
https://raspberrytips.com/mount-usb-drive-raspberry-pi/

UPTIME

Displays the current uptime of the computer or server (how much time on)

Basic usage:	uptime
Last boot date:	uptime -s

CHMOD

Changes file or folder permissions

Digits permissions:	chmod 644 script.sh
Letters permissions:	chmod +x script.sh

NB: Chmod is a complex command for beginner, you can check this tool to know how to read and set permissions correctly:
https://webinpact.com/chmod-calculator/

MAN <COMMAND>

I already give it many times in this document, but man allows finding help for any command

Example:	man find

NB: Press space to go to the next page, and "q" to leave

MISCELLANEOUS COMMANDS

In this part, I want to give you all others useful commands that don't fit into the others categories.

HISTORY

Linux stores any command you type in an archive file, you can read it with "history"

All commands:	history
Last 20:	history | tail -n 20
Clear all history:	history -c
Clear one line:	history -d 123

|

I already show you the pipe in a lot of examples, it allows you to combine multiple commands to find exactly what you want

Syntax:	<command1> | <command2>
Grep example:	cat test.txt | grep error
Double:	du -ak | sort -nr | head -20

!

Run a specific command from the history

Syntax:	!<history_id>
Example:	!123

NB: The history ID changes on each new command you type (including !), make sur to use only once or check the ID again

>

Create a file to store the command output

Syntax:	<command> > <filename>
Example:	cat test.txt | grep error > error.log

NB: The last command put all lines containing "error" in the test.txt file
This command doesn't output anything

CRONTAB

Allows you to schedule tasks on your computer

List current tasks:	crontab -l
Edit tasks:	crontab -e

NB: The crontab syntax is a tough to understand for beginners, use this tool to check your line is correct: https://webinpact.com/crontab-generator/

SCREEN

Run a virtual terminal, to let a session running in background

Start a screen:	screen -S <name>
Exit a screen:	CTRL+A CTRL+D
Resume a screen:	screen -r <name>
Stop a screen:	CTRL+D

!!

Similar to ! but to run the last command again

Usage:	!!

NB: Can be useful to run the same complex commands several times

>>

Add the command output at the end of a file

Usage:	cat test.txt | grep error >> error.log

NB: It's the same usage than >
But in this case, it'll add the lines to the error.log file, and keep the beginning as it was

WARRIORS COMMANDS

And finally, now that you're an expert with a terminal, let's see some tricky commands to push your limits :)
They can be hard to use, with a lot of options, or hard to analyze

- ## AWK

Awk is close to a programming language
Allows you to search string and transform them to display differently

Syntax: `awk [-F] [-v var=value] 'program' file`
Basic example: `awk -F":" '{print $1}' /etc/passwd`

NB: The last command displays only the first column
I can't explain to you the awk usage in detail in a few lines
Check this guide to learn more about this:
https://do.co/2VC8mnm

- ## CUT

Another way to transform text in a command line, probably easier to understand

Syntax: `cut <option> <file>`
Example: `cut -d : -f 1 /etc/passwd`

NB: -d set the delimiter to use, and -f the field to keep
Use "man cut" to learn more about other options

- ## LSOF

Stands for "LiSt Open Files", displays all currently opened files on your computer

Usage: `lsof`

NB: Use grep with a pipe to find the file you're looking for

- ## NETSTAT

Monitors your network activity

Listening ports: `netstat -l`
Add the process ID: `netstat -lp`
Same thing in real-time: `netstat -lpc`

NB: There are many other options for netstat, you can check the "man netstat" page to learn more

- ## SED

Similar to awk, but for regular expressions only

Syntax: `sed <option> <script> <file>`
Basic example: `sed '/^#/d' /etc/apache2/apache2.conf`

NB: The last command remove comments from the configuration
As for awk, you'll need serious tutorials and experience to master this one.

- ## WC

WC stands for "Words Count" and also gets lines count, characters count and file size

Syntax: `wc <options> <file>`
Lines count: `wc -l /var/log/syslog`

NB: -l is for lines, -w for words and -m for characters
You can also use it after a pipe (to count lines from a grep command for example)

- ## WATCH

Monitors a command output, by running it at each specified interval

Basic usage: `watch date`
Specific time: `watch -n10 date`

NB: Default refresh time is 2s

- ## DMESG

Shows a log file of every events happening in the last boot sequence

Usage: `dmesg`

NB: Most of them are normal
You can use grep to look for errors or a specific thing

Thanks for Reading !

See you soon on RaspberryTips
Patrick

RaspberryTips https://raspberrytips.com

Overview

⚠ **OpenVPN is no longer recommended**

We do no longer recommending the use of OpenVPN for new deployments. Although OpenVPN has served us well in the past, we believe it's time to move towards more modern and efficient solutions.

We suggest that users now turn their attention to WireGuard, a forward-thinking VPN solution that offers better performance, faster speeds, and easier implementation. WireGuard has been designed with the latest technology in mind, providing simple yet powerful tools for securing your network communications. Pi-hole's step-by-step tutorial is designed to help you understand the ins and outs of WireGuard, regardless of your technical expertise.

This tutorial is tailored for setting up OpenVPN on a cloud-hosted virtual server (such as Digital Ocean). If you wish to have this working on your home network, you will need to tailor Pi-hole to listen on `eth0` (or similar), which we explain in this section of the tutorial.

High-level Overview

Using a VPN is a responsible, respectful, and safe way to access your Pi-hole's capabilities remotely. Setting up a DNS server has become a simple task with Pi-hole's automated installer, which has resulted in many people knowingly--or unknowingly--creating an open resolver, which aids in DNS Amplification Attacks.

We do not encourage open resolvers but there are always people wanting access to their ad-blocking capabilities outside of their home network, whether it's on their cellular network or on an unsecured wireless network. This article aims to provide a step-by-step walk-through on setting up a server running Pi-hole and OpenVPN so you can connect to your Pi-hole's DNS from anywhere. This guide should work for a private server installed on your private network, but it will also work for cloud servers, such as those created on Digital Ocean.

This tutorial walks you through the installation of Pi-hole combined with a VPN server for secure access from remote clients.

Via this VPN, you can:

- use the DNS server and full filtering capabilities of your Pi-hole from everywhere around the globe
- access your admin interface remotely
- encrypt your Internet traffic

If you don't want a full-tunnel, we provide a page of how to set up your server to exclusively route DNS traffic, but nothing else via the VPN. On another optional page, we describe how to set up Pi-hole + VPN in such a way that it is usable both locally (no VPN) and from remote (through VPN) while preserving full functionality.

In the end, you will have access to a VPN that uses Pi-hole for DNS and tunnels some or all of your network traffic

---

This manual is partially based on this HowTo on Discourse.

Last update: November 30, 2023

Pi-hole®

Network-wide Ad Blocking

INSTALL

SPONSOR US

DONATE

1. Install a supported operating system

You can run Pi-hole in a container, or deploy it directly to a supported operating system via our automated installer.

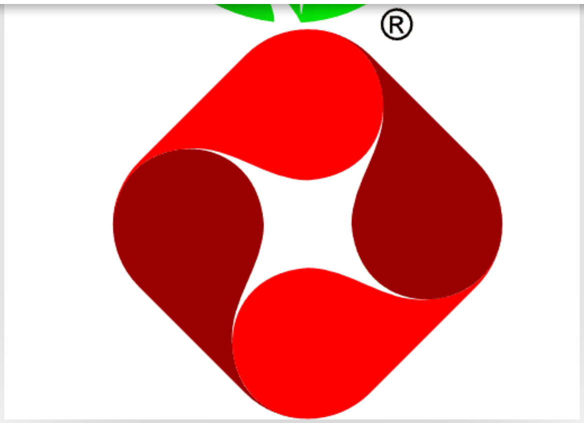
DOCKER INSTALL

SUPPORTED OPERATING SYSTEMS

2. Install Pi-hole

Our intelligent, automated installer asks you a few questions and then sets everything up for you. Once complete, move onto step 3.

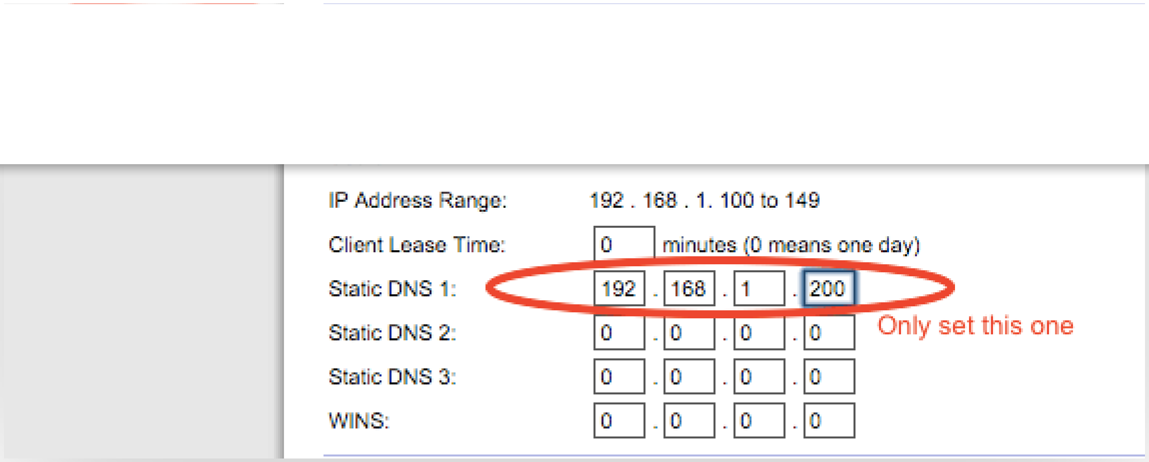
INSTALL PI-HOLE



3. Use Pi-hole as your DNS server

Configure your router’s DHCP options to force clients to use Pi-hole as their DNS server, or manually configure each device to use the Pi-hole as their DNS server.

USE PI-HOLE AS YOUR DNS SERVER



IP Address Range: 192 . 168 . 1. 100 to 149

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 192 . 168 . 1 . 200

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Only set this one

4. Block ads everywhere, even on the go

By pairing your Pi-hole with a VPN, you can have ad blocking on your cellular devices, helping with limited bandwidth data plans.

PI-HOLE + VPN

Network-wide protection

Instead of browser plugins or other software on each computer, **install Pi-hole in one place** and your entire network is protected.

Block in-app advertisements

Network-level blocking allows you to **block ads in non-traditional places** such as mobile apps and smart TVs, regardless of hardware or OS.

Improve network performance

Since **advertisements are blocked *before* they are downloaded**, network performance is improved and will feel faster.

Our Web interface offers control of your Pi-hole and a central place to view statistics. We also include an API for extending these stats.

The Pi-hole Team

The Pi-hole Developers are spread across the globe and work on the project in their spare time. We are a 100% remote-work team.

Dan Schaper

Adam Warner

Dominik Derigs

FTL Designer
Core Developer

Web Interface

In addition to blocking advertisements, Pi-hole has an informative Web interface that shows stats on all the domains being queried on your network.

Built-in DHCP Server

Pi-hole works fine with an existing DHCP server, but you can use Pi-hole’s to keep your network management in one place.

Manage White And Black Lists

Fine-tune your experience by blacklisting or whitelisting domains. Extend this capability with powerful regex statements.

Query Log

See all the domains being queried on your network, where they originated, and more.

Queries are stored in a database and can be queried at any time. Learn about what's happening on your network over time.

Audit Log

Keep track of the most queried domains and add them to a white or blacklist from a central page.

Privacy Modes

Choose from four different privacy modes that works for your environment.

Other Settings

Control and configure other settings from the Web interface.

Post-Install

Making your network take advantage of Pi-hole

Once the installer has been run, you will need to configure your router to have **DHCP clients use Pi-hole as their DNS server** which ensures all devices connected to your network will have content blocked without any further intervention.

If your router does not support setting the DNS server, you can use Pi-hole's built-in DHCP server; just be sure to disable DHCP on your router first (if it has that feature available).

As a last resort, you can manually set each device to use Pi-hole as its DNS server.

Making your Pi-hole host use Pi-hole

Pi-hole will not be used by the host automatically after installation. To have the host resolve through Pi-hole and your configured blocking lists, you can make the host use Pi-hole as upstream DNS server:

> ⚠ **Warning**
>
> If your Pi-hole host is using Pi-hole as upstream DNS server and Pi-hole fails, your host loses DNS resolution. This can prevent successful repair attempts, e.g. by `pihole -r` as it needs a working internet connection.

If your OS uses `dhcpcd` for network configuration, you can add to your `/etc/dhcpcd.conf`

```
static domain_name_servers=127.0.0.1
```

Last update: December 3, 2022

Prerequisites

Hardware

Pi-hole is very lightweight and does not require much processing power

- Min. 2GB free space, 4GB recommended
- 512MB RAM

> **Info**
>
> A Pi-hole branded kit, including everything you need to get started, can be purchased from The Pi Hut, here.

Despite the name, you are not limited to running Pi-hole on a Raspberry Pi. Any hardware that runs one of the supported operating systems will do!

Software

Pi-hole is supported on distributions utilizing systemd or sysvinit!

Supported Operating Systems

The following operating systems are **officially** supported:

Distribution	Release	Architecture
Raspberry Pi OS (formerly Raspbian)	Buster / Bullseye	ARM
Armbian OS	Any	ARM / x86_64 / riscv64
Ubuntu	20.x / 22.x / 23.x	ARM / x86_64
Debian	10 / 11 / 12	ARM / x86_64 / i386
Fedora	36 / 37 / 38	ARM / x86_64
CentOS Stream	8 / 9	x86_64

Info

One of the first tasks the install script has is to determine your Operating System's compatibility with Pi-hole

It is possible that Pi-hole will install and run on variants of the above, but we cannot test them all. If you are using an operating system not on this list you may see the following message:

```
[✗] Unsupported OS detected: Debian 16
  If you are seeing this message and you do have a supported OS, please contact support.

  https://docs.pi-hole.net/main/prerequisites/#supported-operating-systems

  If you wish to attempt to continue anyway, you can try one of the following commands to skip this check:

  e.g: If you are seeing this message on a fresh install, you can run:
         curl -sSL https://install.pi-hole.net | sudo PIHOLE_SKIP_OS_CHECK=true bash

       If you are seeing this message after having run pihole -up:
         sudo PIHOLE_SKIP_OS_CHECK=true pihole -r
       (In this case, your previous run of pihole -up will have already updated the local repository)

  It is possible that the installation will still fail at this stage due to an unsupported configuration.
  If that is the case, you can feel free to ask the community on Discourse with the Community Help category:
  https://discourse.pi-hole.net/c/bugs-problems-issues/community-help/
```

You can disable this check by setting an environment variable named `PIHOLE_SKIP_OS_CHECK` to `true`, however Pi-hole may have issues installing. If you choose to use this environment variable, please use the Community Help topic on Discourse to troubleshoot any installation issues you may (or may not!) have.

IP Addressing

Pi-hole needs a static IP address to properly function (a DHCP reservation is just fine).

On systems that have `dhcpcd5` already installed (e.g Raspberry Pi OS) there is an option in the install process to append some lines to `/etc/dhcpcd.conf` in order to statically assign an IP address. This is an entirely optional step, and offered as a way to lower the barrier to entry for those that may not be familiar with linux systems, such as those first starting out on a Raspberry Pi.

Ports

Service	Port	Protocol	Notes
pihole-FTL	53 (DNS)	TCP/UDP	If you happen to have another DNS server running, such as BIND, you will need to turn it off in order for Pi-hole to respond to DNS queries.
pihole-FTL	67 (DHCP)	IPv4 UDP	The DHCP server is an optional feature that requires additional ports.
pihole-FTL	547 (DHCPv6)	IPv6 UDP	The DHCP server is an optional feature that requires additional ports.
lighttpd	80 (HTTP)	TCP	If you have another Web server already running, such as Apache, Pi-hole's Web server will not work. You can either disable the other Web server or change the port on which `lighttpd` listens, which allows you keep both Web servers running.
pihole-FTL	4711	TCP	FTL is our API engine and uses port 4711 on the localhost interface. This port should not be accessible from any other interface.

Info

The use of lighttpd on port *80* is optional if you decide not to install the Web dashboard during installation. The use of pihole-FTL on ports *67* or *547* is optional, but required if you use the DHCP functions of Pi-hole.

Firewalls

Below are some examples of firewall rules that will need to be set on your Pi-hole server in order to use the functions available. These are only shown as guides, the actual commands used will be found with your distribution's documentation. Because Pi-hole was designed to work inside a local network, the following rules will block the traffic from the Internet for security reasons. `192.168.0.0/16` is the most common local network IP range for home users but it can be different in your case, for example other common local network IPs are `10.0.0.0/8` and `172.16.0.0/12`.

Check your local network settings before applying these rules.

IPTables

IPTables uses two sets of tables. One set is for IPv4 chains, and the second is for IPv6 chains. If only IPv4 blocking is used for the Pi-hole installation, only apply the rules for IP4Tables. Full Stack (IPv4 and IPv6) require both sets of rules to be applied. *Note: These examples insert the rules at the front of the chain. Please see your distribution's documentation for the exact proper command to use.*

IPTables (IPv4)

```
iptables -I INPUT 1 -s 192.168.0.0/16 -p tcp -m tcp --dport 80 -j ACCEPT
iptables -I INPUT 1 -s 127.0.0.0/8 -p tcp -m tcp --dport 53 -j ACCEPT
iptables -I INPUT 1 -s 127.0.0.0/8 -p udp -m udp --dport 53 -j ACCEPT
iptables -I INPUT 1 -s 192.168.0.0/16 -p tcp -m tcp --dport 53 -j ACCEPT
iptables -I INPUT 1 -s 192.168.0.0/16 -p udp -m udp --dport 53 -j ACCEPT
iptables -I INPUT 1 -p udp --dport 67:68 --sport 67:68 -j ACCEPT
iptables -I INPUT 1 -p tcp -m tcp --dport 4711 -i lo -j ACCEPT
iptables -I INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

IP6Tables (IPv6)

```
ip6tables -I INPUT -p udp -m udp --sport 546:547 --dport 546:547 -j ACCEPT
ip6tables -I INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

FirewallD

Using the `--permanent` argument will ensure the firewall rules persist reboots. If only IPv4 blocking is used for the Pi-hole installation, the `dhcpv6` service can be removed from the commands below. Create a new zone for the local interface (`lo`) for the pihole-FTL ports to ensure the API is only accessible locally. Finally `--reload` to have the new firewall configuration take effect immediately.

```
firewall-cmd --permanent --add-service=http --add-service=dns --add-service=dhcp --add-service=dhcpv6
firewall-cmd --permanent --new-zone=ftl
firewall-cmd --permanent --zone=ftl --add-interface=lo
firewall-cmd --permanent --zone=ftl --add-port=4711/tcp
firewall-cmd --reload
```

ufw

ufw stores all rules persistent, so you just need to execute the commands below.

IPv4:

```
ufw allow 80/tcp
ufw allow 53/tcp
ufw allow 53/udp
ufw allow 67/tcp
ufw allow 67/udp
```

IPv6 (include above IPv4 rules):

```
ufw allow 546:547/udp
```

Last update: October 1, 2023

RASPBERRY PI

The 24 Best Games For Retro gaming systems

"It's difficult to find good games available on Retropie with an available download link I'll give you a list of my favorite games with a screenshot I took and a download link for each one" - RaspberryTips.com

RaspberryTips

Best games for Retropie / RecalBox / Lakka

DONKEY KONG

Let’s start with a mythic game from the 80s: Donkey Kong
For the youngest, you probably know more recent adventures of Donkey Kong, so I give you the link to the Nintendo 64 version, with better graphics :)

Information

Platform
Nintendo 64

Release Date
November 22, 1999

Download
romhustler.net

SUPER BOMBERMAN 5

Bomberman is a classic puzzle / maze game
Super Bomberman 5 is nonlinear, giving players a choice of which level they'd like to complete next. These phases are all based on the four previous Super Bomberman games for the Super Famicom

Information

Platform
Super Nintendo

Release Date
February 28, 1997

Download
romhustler.net

WAVE RACE

Wave Race 64 is a jet ski racing game
There are several game modes like Championship, Time trial or Stunt mode
You can play each mode solo or multiplayer

Information

Platform
Nintendo 64

Release Date
September 27, 1996

Download
romhustler.net

DOOM

Doom is a 1993 first-person shooter video game by id Software for MS-DOS. It is considered one of the the most significant and influential titles in video game history

Information

Platform
Super Nintendo

Release Date
December 10, 1993

Download
romhustler.net

Best games for Retropie / RecalBox / Lakka (2)

STREET FIGHTER II

This one is a monument
Street Fighter II Turbo was a bestseller in the 90s.
I think it's the best version from the Street Fighter series
I present here the SNES version, but you should know that they adapted it after that for a lot of other platforms

Information

Platform
Super Nintendo

Release Date
February 1991

Download
romhustler.net

OUTRUN

Outrun is an arcade game released by Sega in September 1986. It is known for its pioneering hardware and graphics and innovative features such
as nonlinear gameplay and a selectable soundtrack
I have great memories of this game

Information

Platform
Mega Drive

Release Date
September 25, 1986

Download
romhustler.net

GOLDEN EYE 007

Like Wave Race 64 and Super Mario 64, it was one of the games I played the most: Golden Eye 007
From the movie of the same name, you play James Bond in a series of adventures in URSS
This game was one of the first to bring so much reality in first person video games

Information

Platform
Nintendo 64

Release Date
August 25, 1997

Download
romhustler.net

SIM CITY 2000

SimCity 2000 is a city-building simulation video game and the second installment in the SimCity series
SimCity 2000 was a major extension of the concept, with budget and finance controls, new buildings and a new underground layer for water pipes and subways

Information

Platform
Nintendo 64

Release Date
1993

Download
romhustler.net

Best games for Retropie / RecalBox / Lakka (3)

PACMAN

Pacman is a mythic game, you already know it

First available in arcade rooms in 1980, Pacman was then developed on a lot of classic platforms (like Atari, SNES, PlayStation and Game Boy)

Pacman is also often used as a reference in books and movies (Pixels, Player One, Black Mirror, ...)

Information

Platform
Game Gear

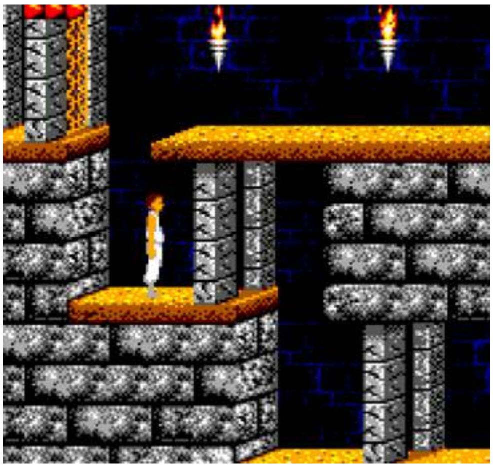
Release Date
October 26, 1980

Download
romhustler.net

PRINCE OF PERSIA

Prince Of Persia is a series of action-aventure games focused on various incarnations of the prince.

I remember playing Prince of Persia on an Amstrad computer, but here is the MasterSystem version, fully compatible with all retro gaming systems



Information

Platform
Sega MasterSystem

Release Date
October 3, 1989

Download
romhustler.net

SONIC THE HEDGEHOG

Sonic The Hedgehog is one of the biggest success stories in gaming

Available for over than 25 different platforms and not counting how many game versions

You lead the small blue hedgehog through an adventure in a lot of different levels

Information

Platform
Megadrive

Release Date
June 23, 1991

Download
romhustler.net

CONTRA

Contra is a run and gun video game developed and published by Konami

The default weapon is a rifle with unlimited ammunition that can be upgraded into other guns

The game can be played by up to two players

Information

Platform
Nintendo

Release Date
February 20, 1987

Download
romhustler.net

Best games for Retropie / RecalBox / Lakka (4)

DUCK HUNT

Take this dog out of my sight!
Duck Hunt is a famous game where you need to kill ducks with a gun controller
If you have already played this game, you should remember

Information

Platform
Nintendo

Release Date
April 21, 1984

Download
romhustler.net

PAPERBOY

The player takes the role of a paperboy who delivers a fictional newspaper called "The Daily Sun" along a suburban street on his bicycle.

Information

Platform
Nintendo 64

Release Date
1980

Download
romhustler.net

TONY HAWK

Oh, my god … I don't know how many hours I spent on this game: Tony Hawk Pro Skater
I mainly played this game on PlayStation (1/2), but it was also available on Nintendo systems and PC
My favorite mode is the Career mode where you start with a noob and improve your stats to challenge pro skaters

Information

Platform
Nintendo 64

Release Date
August 31, 1999

Download
romhustler.net

WIPEOUT 64

Wipeout 64 is a futuristic racing game
Wipeout is based on a futuristic anti-gravity setting where pilots would race against each other or computer-controlled AI opponents to finish in the highest position possible

Information

Platform
Nintendo 64

Release Date
November 10, 1998

Download
romhustler.net

Best games for Retropie / RecalBox / Lakka (5)

SENSIBLE SOCCER

Yeah ... Football gaming looked like that in the beginning of the 90s
The first FIFA didn't exist yet and we had to play with 10 pixels players
It's an historical game, but I doubt you'll spend your afternoon on this game today

Information

Platform
Megadrive

Release Date
1992

Download
romhustler.net

WORMS ARMAGEDDON

Worms Armageddon is a 2D artillery turn-based tactics video game developed by Team17 and part of the Worms series. The player controls a team of up to eight worms in combat against opposing teams either AI- or player-controlled, using fun weapons

Information

Platform
Nintendo 64

Release Date
1999

Download
romhustler.net

LOTUS TURBO CHALLENGE

Lotus Turbo Challenge is a racing / driving game, available on Genesis, Amiga and Atari ST
The decor is minimalist, but I remember spending a lot of time on this one
The Lotus cars company inspired this game

Information

Platform
Sega Mega Drive

Release Date
1991

Download
romhustler.net

RAYMAN 2

Rayman is a classic platform series

The game is often mentioned in some "Best Games Of All Time" lists, so I have to put it on this list

Information

Platform
Nintendo 64

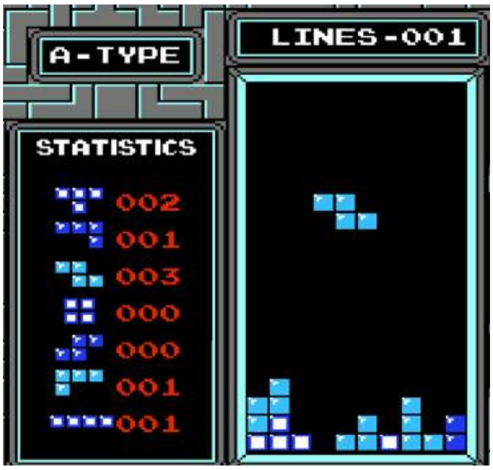
Release Date
October 29, 1999

Download
romhustler.net

Best games for Retropie / RecalBox / Lakka (6)

TETRIS

How to make a retro gaming compilation without Tetris? Impossible
I know you like this game and you played it on many systems from Game Boy to PC
As everyone already knows this game, I have nothing to add ;)



Information

Platform
Nintendo

Release Date
June 6, 1984

Download
romhustler.net

ZELDA: LINK TO PAST

I finally found a Zelda version available on the Internet, and not the worst :)
"The Legend of Zelda: A Link to the Past" is an action-adventure video game developed by Nintendo for the SNES video game console
Link travels on a journey to save Hyrule, defeat Ganon and rescue maidens related to the Sages

Information

Platform
Nintendo 64

Release Date
November 21, 1991

Download
gamulator.com

LEMMINGS

Lemmings is a puzzle game, where lemmings fall from the top of the screen and you need to bring them to the exit without losing too much of them
To do this, you have several actions available like climbing, digging or blocking others (to make them change direction)

Information

Platform
Super Nintendo

Release Date
1991

Download
romhustler.net

MARIO KART 64

Last but not least, you probably expected it, here is the only Mario game I put in this list, exclusively on PDF, because I'm not sure of the legal aspect
But Gamulator offers it on their website, so enjoy :)
I don't think I have something more to add about this game ^^

Information

Platform
Nintendo 64

Release Date
December 14, 1996

Download
gamulator.com

Raspberry Pi Commands Cheat Sheet

74 Raspberry Pi Commands

From

RaspberryTips

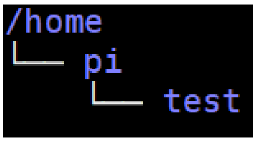
FILES MANAGEMENT

These commands are the basics that every Linux beginner should learn to browse the Linux files tree from a terminal

Reminder:

The Linux files organization is a tree, starting at /
Each subfolder adds a new level under /

For example, on the image you can see the tree for this folder : /home/pi/test



```
/home
└── pi
    └── test
```

CD <FOLDER>

Changes directory, go to the specified folder

Absolute path:	cd /home/pi/test
Relative path:	cd test

NB: "Absolute" is when you use the entire path
For "relative" you only enter the path from your current directory (in the second example, you need to already be in the /home/pi folder)

MKDIR <FOLDER>

Creates a new subfolder in the current or specified path

Current directory:	mkdir test
Specific:	mkdir /home/pi/test

NB: The first example create a folder in your current directory (relative path)
The second one create a new directory in the exact parameter (absolute path)

MV <SRC> <TARGET>

Moves a file or directory to another location (cut/paste)

Move a file:	mv test.txt /home/pi
Move a folder:	mv /home/pi/test /home/pi/test2

NB: The mv command is always in recursive mode

MORE <FILENAME>

Displays the content of the file, page per page, from the beginning

Absolute path:	more test.txt
Relative path:	more /home/pi/test.txt

NB: For long files, you need to press "space" to continue, or "q" to quit

LS (FOLDER)

Lists files and directory, in the current or specified folder

Current directory:	ls
Specific:	ls /home/pi/test

NB: You can use options with ls to get a more detailed view of files and folder, ex: ls -latr /home/pi

CP <SOURCE> <TARGET>

Copies a file or directory to another location (copy/paste)

Copy a file	cp test.txt /home/pi
Recursive copy:	cp -r /home/pi/test /home/user/

NB: Use the recursive option to copy a folder and all its files and folders

CAT <FILENAME>

Displays the content of the file, without pagination

Display on file:	cat test.txt
Use pattern:	cat *.txt

NB: A pattern allows you to display all files content for similar files

TAIL <FILENAME>

Displays the end of the file

Basic usage:	tail test.txt
Lines count:	tail -n20 test.txt
Real-time display:	tail -f test.txt

NB: The -n option allows you to ask for a specific number of lines to display
The -f option refresh the display each time the file is modified (perfect for log files monitoring)

FILES MANAGEMENT (2)

HEAD <FILENAME>

Similar to tail but to display the beginning of the file

Display 10 lines:	head test.xt
With lines count:	head -n20 test.txt

TOUCH <FILENAME>

Create a new empty file

Current directory:	touch test.txt
Specific:	touch /home/pi/test.txt

NB: Most of the time, nano is a better choice to create a file, as you can edit it directly

GREP

Grep is a powerful (and complex) tool to search string in a text or file

<table>
<tr><td><em>Find string in a file</em></td><td>grep "dhcp" /var/log/syslog</td></tr>
<tr><td><em>Filter a command output</em></td><td>ls -latr | grep ".php"</td></tr>
<tr><td><em>With a script:</em></td><td>/home/pi/script.sh | grep error</td></tr>
</table>

NB: The | option (pipe), allows you to run a command on another one output
You need to use quotes for complex search with space or special characters

There are also advanced usages possible:

<table>
<tr><td><em>Regular expressions:</em></td><td>grep "dhcp\|dns" /var/log/syslog</td></tr>
<tr><td><em>Command options:</em></td><td>grep -A2 -B4 'Fatal error' /var/log/syslog</td></tr>
<tr><td><em>Inverted search:</em></td><td>grep -v 'Notice' /var/log/syslogi</td></tr>
</table>

The | in the regular expressions allows you to use OR (one or more condition)
The -A option also catch X lines "after" the matched condition, -B is for "before"
Finally, the -v option is to filter lines that don't match the condition

NANO <FILENAME>

Opens and edit the specified file. Nano is a powerful text editor in a terminal

Basic usage:	nano /home/pi/test.txt

NB: Nano will create the file if it doesn't exist

RM <FILENAME>

Removes a file or directory

Remove file:	rm test.txt
Remove directory:	rm -rf /home/pi/test

NB: You need to use -rf options to remove a directory even if not empty (recursive + force)

TAR

Tar is the linux way to manage compressed files

Create a new archive:	tar -cvfz archive.tar.gz /home/pi/test
Extract files	tar -xvfz archive.tar.gz

Options:
-c is to Compress, -x to eXtract
-v: verbose mode, -z: use gZip to compress, -f specify the file name
Use "man tar" for more information

ZIP / UNZIP

Zip is similar to tar, but mainly used on Windows systems

Create a new archive:	zip -r archive.zip /home/pi/test
Extract files:	unzip archive.zip

NB: The -r option is to compress all the folder content
You can use the -d option to extract files in a specific folder
Use "man zip" or "man unzip" for all available options

FILES MANAGEMENT (3)

PWD

An easy command to display you current directory

Example:	pwd

TREE

Another tool to get details on your current location, in a tree format

Current directory:	tree
Specific folder:	tree /home/pi/

NB: There are a few options to filter the output, by selecting only directory, managing symbolic links or setting a max depth level

FIND

Find allows you to search files on your Raspberry Pi, there is a lot of options

Find a file name:	find /home/pi -iname test.txt
Filter extensions:	find /home/pi -iname *.php
Find only directories:	find / -type d -iname test

NB: -iname stands for "insensitive case", you can use -name if you prefer
You can use "-type f" to find only files

More advanced options:

File size:	find / -size +10M
Recently modified files:	find /home -mtime -2

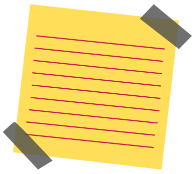
Run command on results:

```
find /var/log -iname *.log.gz -exec rm {} \;
```

The first command display all files over 10M on the disk
The -mtime -2 checks files modified in the last two days
The {} parameter in the last command will be replaced by the file name
Check the "man find" for more information

NETWORK COMMANDS

Here are the main commands to know to manage and use the network on your Raspberry Pi



Reminder:

Recent Raspberry Pi models comes with two interfaces : Ethernet and Wifi
Ethernet is called eth0 and the Wifi one is wlan0

IFCONFIG

Displays your current network configuration (IP Address, Mac Address, ...)

Usage:

```
ifconfig
```

NB: You can add an interface name to display only this one, for example: "ifconfig wlan0"

IWCONFIG

Shows information about the wireless network configuration (SSID, speed, ...)

Usage:

```
iwconfig
```

NB: You can also display a specific interface with iwconfig wlan0

IFUP / IFDOWN

Allows you to enable or disable one specific interface

Enable interface:

```
sudo ifup eth0
```

Disable interface:

```
sudo ifdown eth0
```

NB: It can help to disable the wireless interface while connected by cable

PING <HOST>

Checks if the host is alive

Basic usage:

```
ping 192.168.1.1
```

NB: Read the "man ping" to see all available options

HOSTNAME

Displays or set the Raspberry Pi hostname

Display hostname:

```
hostname
```

Set a new hostname:

```
sudo hostname RaspberryZero
```

WGET <URL>

Download a file with the terminal

Basic usage:

```
wget http://192.168.1.1/test.txt
```

Change file name:

```
wget http://192.168.1.1/test.txt -O  target.txt
```

SSH <USER>@<IP>

Connects to another Linux system with SSH

Example:

```
ssh pi@192.168.1.1
```

SCP

Copies a file over the network by using SSH

Syntax:

```
scp <file> <user>@<ip>:<path>
```

Example:

```
scp test.txt pi@192.168.1.1:/home/pi/
```

RSYNC

Similar to SCP with more options like delta comparison and some other optimizations

Syntax:

```
rsync <file> <user>@<ip>:<path>
```

Example:

```
rsync test.txt pi@192.168.1.1:/home/pi/
```

Local copy:

```
rsync /home/pi/* /media/usb/
```

Remote recursive copy:

```
rsync -auzr /home/pi/Documents/* pi@192.168.1.1:/home/pi/Documents/
```

NB: Use "man rsync" to get all possible options

RaspberryTips https://raspberrytips.com

PACKAGES MANAGEMENT

Once you have the network working, you'll probably update your system and install needed package
On this page, you have all the required commands to do this from a terminal

Vocabulary:

On Linux, each software is a **package**, as well as each **dependency**
You are downloading new packages from **repositories** (servers hosting packages)
You need to use a tool called **apt** to search, install and updates packages on Debian/RPI OS
All these commands need root privilege, you have to use sudo before each one

APT UPDATE

Downloads the last packages list from your repositories

Usage:

```
sudo apt update
```

NB: To add a new repository, you can edit the apt configuration in /etc/apt/sources.list, or follow the instructions from the software editor

APT UPGRADE

Downloads and installs the latest version of each package available in the repository

Usage:

```
sudo apt upgrade
```

NB: You need to run apt update before doing this, to get the latest versions
The -y option allows you to automatically accept the installation

RPI-UPDATE

Updates everything on your Raspberry Pi, use with precaution

Usage:

```
sudo rpi-update
```

APT INSTALL <PACKAGE>

Installs the specified package on your system

Usage:

```
sudo apt install phpmyadmin
```

NB: Use the following search command to know the exact name of a package

APT REMOVE <PACKAGE>

Uninstall a package from your system

Usage:

```
sudo apt remove vim
```

NB: I give you the command to list currently installed packages in the next line

APT SEARCH

Very useful to find the exact package name before installing it

Usage:

```
apt search openjdk
```

With grep:

```
apt search openjdk | grep jre
```

NB: You don't need sudo for this one

MANUAL INSTALLATION

Sometimes, you need to install packages manually, if the editor doesn't provide a repository

Download the file with wget:

```
wget https://www.realvnc.com/download/file/viewer.files/VNC-Viewer-6.19.325-Linux-ARM.deb
```

Manual installation:

```
sudo dpkg -i VNC-Viewer-6.19.325-Linux-ARM.deb
```

NB: You can use dpkg -r to remove a package manually, or dpkg-reconfigure to redo the configuration after installation

LIST INSTALLED PACKAGES

Dpkg can also be useful to list currently installed packages

Syntax:

```
dpkg -l
```

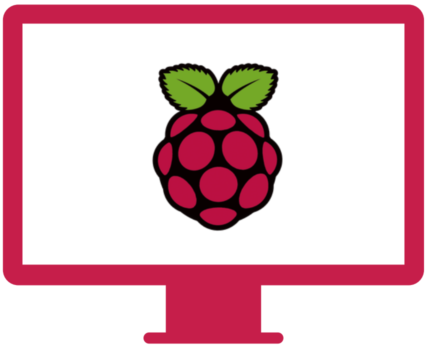
With grep:

```
dpkg -l | grep php
```

NB: Read the "man dpkg" output to get all possible options from this command

SYSTEM MANAGEMENT

Now that you have all packages installed, you may need to learn more advanced commands on how to manage your Raspberry Pi operating system



REBOOT

This command will restart your Raspberry Pi immediately

Usage:	sudo reboot

SERVICE

Each daemon has an associated service, you can start or stop it when you want

Start:	sudo service apache2 start
Stop:	sudo service apache2 stop
Restart:	sudo service apache2 start
Reload config:	sudo service apache2 reload

NB: Use "service <service>" to list all available options, for example "service apache2"
The tab key will help you to find the service name

PROCESS LIST

Displays all running processes

Basic usage:	ps aux
Only by a specific user:	ps -u pi

NB: I give you the command to list currently installed packages in the next line

HTOP

A great alternative to top, to display system load and process in an intuitive interface

Usage:	htop

NB: htop is not installed by default, install it with "apt install htop"

SHUTDOWN

Stops the Raspberry Pi, now or at a specific time

Stop now:	sudo shutdown -h now
At a specific time:	sudo shutdown -h 20:00

START SERVICE ON BOOT

Most of the time, services automatically start on boot, but if needed you can do this manually

Start on boot:	sudo update-rc.d ssh enable
Don't start on boot:	sudo update-rc.d -f ssh remove

NB: To start a script on boot, add it to the /etc/rc.local file

KILL / KILLALL

Immediately stop a specific process or all processes from the same command

Kill:	kill 12345
Killall:	killall php

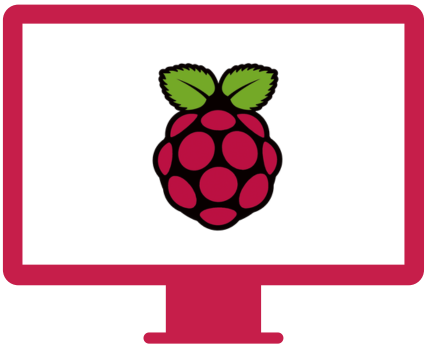
NB: Use the ps command to find the process ID to kill

DF

Displays your partition list, a good way to check the remaining disk space

Basic usage:	df
More readable:	df -h
Specific partition:	df -h /media/usb

SYSTEM MANAGEMENT (2)



DU

Displays the disk space usage in the current or specified folder

Basic usage:	du
Specific folder:	du /home/pi
Summarize:	du --summarize /home/pi
20 biggest files:	du -ak | sort -nr | head -20

NB: There are a lot more options, check the "man du" to find more help about this one

DATE

As the name says, display the current date and time

Full output:	date
Specific format:	date +%m-%d-%Y

NB: The "man date" command gives you the list of all availables options and format

CHOWN

Changes file owner and group

Change file owner:	sudo chown pi /usr/local/bin/script.sh
Change file owner & group:	sudo chown pi:www-data /var/www/html/mysite

CPU TEMPERATURE

It's not an easy command to remember, but very useful while overclocking or running consuming apps

Usage:	vcgencmd measure_temp

NB: vcgencmd is hidden in the libraspberrypi-bin package, you may need to install it manually on Raspberry Pi OS lite: "sudo apt install libraspberrypi-bin"

MOUNT

Mount a new partition (usb key for example)

Mount disk:	sudo mount /dev/sda1 /mnt/usb
Unmount:	sudo umount /mnt/usb

NB: It's a complex command for beginner, but this post will give you all the needed informations https://raspberrytips.com/mount-usb-drive-raspberry-pi/

UPTIME

Displays the current uptime of the Raspberry Pi (how many time on)

Basic usage:	uptime
Last boot date:	uptime -s

CHMOD

Changes file or folder permissions

Digits permissions:	chmod 644 script.sh
Letters permissions:	chmod +x script.sh

NB: Chmod is a complex command for beginner, you can check this tool to know how to read and set permissions correctly: https://chmod-calculator.com/

MAN <COMMAND>

I already give it a lot of times in this document, but man allows finding help on a command

Example:	man find

NB: Press space to go to the next page, and "q" to leave

RASPBERRY PI OS COMMANDS

As a Debian-like operating system, RPI OS use most of the same commands
But you'll find here the specific RPI OS commands

Note:

There are a few commands that only works on Raspberry Pi OS
They are not essentials to use a Raspberry Pi (except the first one probably)
But on most websites you'll not find them as they are not present on other Linux distributions

RASPI-CONFIG

This is the main tool to configure your Raspberry Pi from a terminal

Usage:

```
sudo raspi-config
```

NB: Raspi-config allows you a lot of changes in your Raspberry Pi configuration, like password, network options, boot options, localisation options, interfacing options (ssh), overclocking and other advanced options

LIBCAMERA-VID

It's the same thing but to capture video from your camera

Basic usage:

```
libcamera-vid -o video.h264 -t 10000
```

NB: -t option is for the time you want to capture the video
You'll find all needed information on how to use your camera on this post :
https://raspberrytips.com/camera-raspberry-pi/

RPI-UPDATE

We already saw this command in the system updates section, it'll update everything on your system

Usage:

```
sudo rpi-update
```

LIBCAMERA-STILL

This command allows you to take a picture from the Raspberry Pi camera

Basic usag

```
libcamera-still -o image.jpg
```

NB: You'll find all needed informations on how to use your camera on this post :
https://raspberrytips.com/camera-raspberry-pi/

RASPI-GPIO

Set or get values from your GPIO pins in a terminal

Get value:

```
sudo raspi-gpio get
```

Set value:

```
sudo raspi-gpio set 20 a5
```

NB: It can be a good start to check that your circuit is working, but the best way is to use Python scripts, more info here:
https://raspberrytips.com/raspberry-pi-gpio-pins/

MISCELLANEOUS COMMANDS

In this part, I wanted to give you all others useful commands that doesn't fit into the others

HISTORY

Linux stores any command you type in an archive file, you can read it with "history"

All commands:	history
Last 20:	history | tail -n 20
Clear all history:	history -c
Clear one line:	history -d 123

|

I already show you the pipe in a lot of examples, it allows you to combine multiple commands to find exactly what you want

Syntax:	<command1> | <command2>
Grep example:	cat test.txt | grep error
Double:	du -ak | sort -nr | head -20

!

Run a specific command from the history

Syntax:	!<history_id>
Example:	!123

NB: The history ID changes on each new command you type (including !), make sur to use only once or check the ID again

>

Create a file to store the command output

Syntax:	<command> > <filename>
Example:	cat test.txt | grep error > error.log

NB: The last command put all lines containing "error" in the test.txt file
This command doesn't output anything

CRONTAB

Allows you to schedule tasks on your Raspberry Pi

List current tasks:	crontab -l
Edit tasks:	crontab -e

NB: The crontab syntax is a tough to understand for beginners, use this tool to check your line is correct:
https://crontab.guru/

SCREEN

Run a virtual terminal, to let a session running in background

Start a screen:	screen -S <name>
Exit a screen:	CTRL+A CTRL+D
Resume a screen:	screen -r <name>
Stop a screen:	CTRL+D

!!

Similar to ! but to run the last command again

Usage:	!!

NB: Can be useful to run the same complex commands several times

>>

Add the command output at the end of a file

Usage:	cat test.txt | grep error >> error.log

NB: It's the same usage than >
But in this case, it'll add the lines to the error.log file, and keep the beginning as it was

WARRIORS COMMANDS

And finally, now that you're an expert with a terminal, let's see
some tricky commands to push your limits :)
They can be hard to use, with a lot of options, or hard to analyze

AWK

Awk is close to a programming language
Allows you to search string and transform them to display differently

Syntax: awk [-F] [-v var=value] 'program' file
Basic example: awk -F":" '{print $1}' /etc/passwd

NB: The last command displays only the first column
I can't explain to you the awk usage in detail in a few lines
Check this guide to learn more about this:
https://do.co/2VC8mnm

CUT

Another way to transform text in a command line, probably easier to understand

Syntax: cut <option> <file>
Example: cut -d : -f 1 /etc/passwd

NB: -d set the delimiter to use, and -f the field to keep
Use "man cut" to learn more about other options

LSOF

Stands for "LiSt Open Files", displays all currently opened files on your Raspberry Pi

Usage: lsof

NB: Use grep with a pipe to find the file you're looking for

NETSTAT

Monitors your network activity

Listening ports: netstat -l
Add the process ID: netstat -lp
Same thing in real-time: netstat -lpc

NB: There are many other options for netstat, you can check the "man netstat" page to learn more

SED

Similar to awk, but for regular expressions only

Syntax: sed <option> <script> <file>
Basic example: sed '/^#/d' /etc/apache2/apache2.conf

NB: The last command remove comments from the configuration
As for awk, you'll need serious tutorials and experience to master this one.

WC

WC stands for "Words Count" and also gets lines count, characters count and file size

Syntax: wc <options> <file>
Lines count: wc -l /var/log/syslog

NB: -l is for lines, -w for words and -m for characters
You can also use it after a pipe (to count lines from a grep command for example)

WATCH

Monitors a command output, by running it at each specified interval

Basic usage: watch date
Specific time: watch -n10 date

NB: Default refresh time is 2s

DMESG

Shows a log file of every events happening in the last boot sequence

Usage: dmesg

NB: Most of them are normal
You can use grep to look for errors or a specific thing

Thanks for Reading !

See you soon on RaspberryTips
Patrick

RaspberryTips

The Raspberry Pi Glossary

Word	Explanation
APT	Advanced Package Tool. The software manager used on Raspberry Pi to install updates new applications.
ARM	A low-cost and minimal power consumption architecture for computer processors, used on all the Raspberry Pi models.
CLI	Command Line Interface. The black screen where we can only use Linux commands to interact with the operating system.
CPU	Central Processing Unit. Basically, the processor, the primary component of a computer to run everything.
DHCP	Dynamic Host Configuration Protocol. Networking service which automatically assign an IP address to each new device on the network.
Distribution	A Linux operating system version, using a specific set of software. Ex: Raspberry Pi OS, Ubuntu, Debian.
DNS	Domain Name System. A system or service which translates domain names to IP addresses, the only identifier understood by computers.
Etcher	Balena Etcher is a tool to copy the operating system files on a specific device (in general: USB or SD card).
Ethernet	A networking technology. Generally used to identify the wired connection or port on a Raspberry Pi.
Firmware	The basic software controlling the low-level operations for a specific hardware.
Flash	The action to copy the operating system files to a SD card with Etcher, Raspberry Pi Imager or any other tool.
GPIO	General Purpose Input Output. The Raspberry Pi include a 40 GPIO pins on each board, to create an electronic circuit and use extension cards (HAT).
GPU	Graphic Processing Unit. The equivalent of the CPU to handle all the graphical part (display, video processing, etc).
GUI	Graphical User Interface. Opposite of CLI. Mouse and graphical tools are available to make the device management easier.
HAT	Hardware Attached on Top. Extension cards that can be plugged on the GPIO ports of a Raspberry Pi.
HDMI	High-Definition Multimedia Interface. The main display interface on Raspberry Pi. Recent models are using different variants (Mini or Micro-HDMI ports).

The Raspberry Pi Glossary

Headless	A term used to define the use of a Raspberry Pi without any screen.
Hostname	A name assigned to a device on a network.
I2C	Inter Integrated Circuit. Several GPIO pins are reserved for I2C devices. It's a specific bus to connect compatible peripherals.
IP Address	Unique identifier for a device on a network. Ex: 192.168.1.10
LAN	Local Area Network. Generally refers to your network at home. Opposite to a WAN (Wide Area Network) that we use to speak about the Internet.
LibreOffice	A complete office suite, including a word processor and spreadsheet (free alternative to Microsoft Office)
Linux	A family of open-source operating system using the Linux kernel, the base of all the Linux distributions.
MAC Address	Media Access Control Address. A unique identifier assigned to each network card. Can be used in a DHCP server to reserve an IP address to each device.
NOOBS	New Out-Of-the-Box Software. It was the basic software pre-installed on most SD card for Raspberry Pi to install an operating system. Obsolete, no longer developed.
OS	A software that manages everything on a computer (hardware, resources, software, services). Ex: Windows, macOS, Linux.
Partition	One segment of a storage device (hard drive or SD card) that we allocate to a specific usage. Ex: / and /boot are the main partitions on a Raspberry Pi.
PIXEL	A desktop environment, based on LXDE and adapted for the Raspberry Pi. Now referred as "Raspberry Pi Desktop".
Python	A popular programming language, pre-installed on Raspberry Pi OS.
RAM	Random Access Memory. A temporary and fast storage type present on any computer. In general, the more RAM you have, the faster your programs will run. It's also better to use several apps simultaneously.
Raspberry Pi OS	A Linux distribution especially tailored for the Raspberry Pi. It's the default operating system, based on Debian.
Raspbian	Obsolete. The name of the default Linux distribution before Raspberry Pi OS (same thing, they only changed the name).
Raspi-config	A tool available on Raspberry Pi OS to configure the system from a terminal.
Repository	A server or group of servers on the Internet hosting the software files used by the package manager. Each Linux distribution have several repositories.

The Raspberry Pi Glossary

Root	The name of the administrator account on Linux systems.
Scratch	A visual programming language and tool. Pre-installed on Raspberry Pi OS with Desktop, and intended to help kids to learn how to code without the hassle of the programming syntax.
SD card	Secure Digital card. The main storage device on Raspberry Pi (microSD card in fact).
SPI	Serial Peripheral Interface bus. Similar to I2C, another way to communicate with compatible peripherals via some GPIO pins.
Splash screen	The image or graphical element displayed on boot by most operating systems. Can also refer to the same thing for an application (Ex: Gimp, PyCharm and Photoshop have a splash screen).
SSD	Solid-State Drive. A storage device, faster than the usual HDD, and also the SD cards. Can be used as the main storage on recent Raspberry Pi models (instead of the SD card).
SSH	Secure Shell Protocol. A network protocol used to remotely access a computer (a Raspberry Pi for example). This allows to access the Raspberry Pi terminal from another device.
sudo	Stands for "super user do!". Allow us to run commands with administrator privileges from an authorized used session. Ex: the "pi" user can use sudo instead of switching to "root".
Underscan	A setting allowing us to adjust the display to the screen size. Disable it if you have black bars that appear on the sides of your screen. Opposite: overscan.
VNC	Virtual Network Computing. A remote access software, pre-installed on Raspberry Pi OS. Allow us to control the Raspberry Pi desktop environment from another computer.

Python Cheat Sheet

Variables

```
name = 'Patrick'
height = 182
old = true
```

Print, concatenation, comments

```
#This is a comment
print("Hello world")
print("Hello " + name)
```

Conditions

```
a == b
a != b
a < b
a > b
a <= b
a >= b
a = true
```

```
if a > 0:
   print("First case")
elif b > 0:
   print("Second case")
else:
   print("Default")
```

```
if a > 0 and b > 0:
   print("And")
elif a > 0 or b > 0:
   print("Or")
```

Loops

```
i = 1
while i < 5:
   print(i)
   i += 1
```

```
alphabet= ["a", "b", "c"]
for letter in alphabet:
  print(letter)
```

Functions

```
def say_hello(name):
   print("Hello " + name)

say_hello("Patrick")
```

Modules

```
import time
from time import sleep
```

Built-in functions

```
len(string)
format(value, format)
isinstance(object, type)
str(object)
int(value)
range(min, max, step)
```

```
open(filename, mode)
type(object)
exec(code)
float(value)
min(value), max(value)
round(value)
```

FAQ

[VPN] How to set up a VPN server on ASUS router – PPTP

Last Update : 2023/10/26 11:43

SEND TO EMAIL | OPEN ON YOUR SMART PHONE

[VPN] How to set up a VPN server on ASUS router – PPTP

1. Some functions of VPN will be different due to firmware version

Interface 1: Supports routers with firmware later than 3.0.0.4.388.xxxx (including), please refer to here for the s

instructions.

Interface 2: Supports routers with firmware earlier than 3.0.0.4.388.xxxx, please refer to here for the setting inst

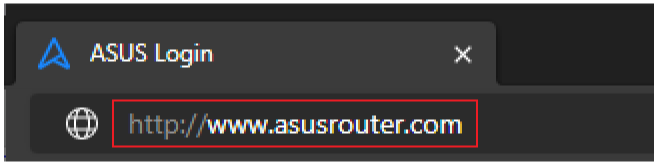
2. For information on how to upgrade the firmware, please refer to the FAQ [Wireless Router] How to update th firmware of your router to the latest version

3. FAQ

Interface 1

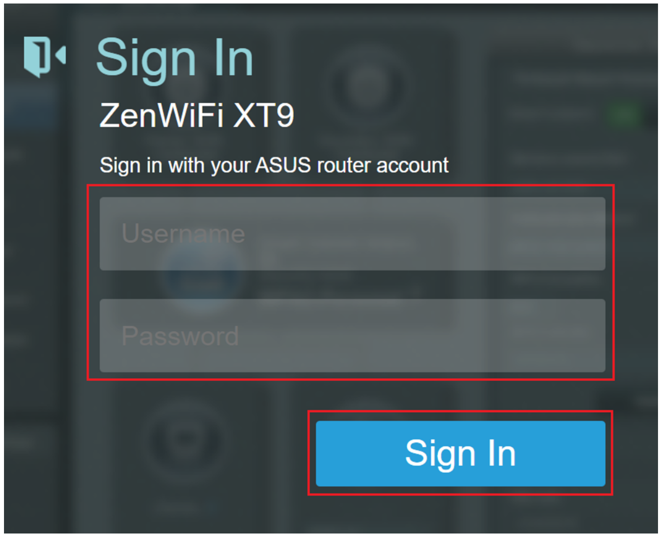
Please follow the steps below to set up a VPN server - PPTP on your ASUS router.

1. Connect your computer to the router via wired or WiFi connection and enter your router LAN IP or router URI http://www.asusrouter.com to the WEB GUI.



Note: Please refer to How to enter the router setting page(Web GUI) to learn more.

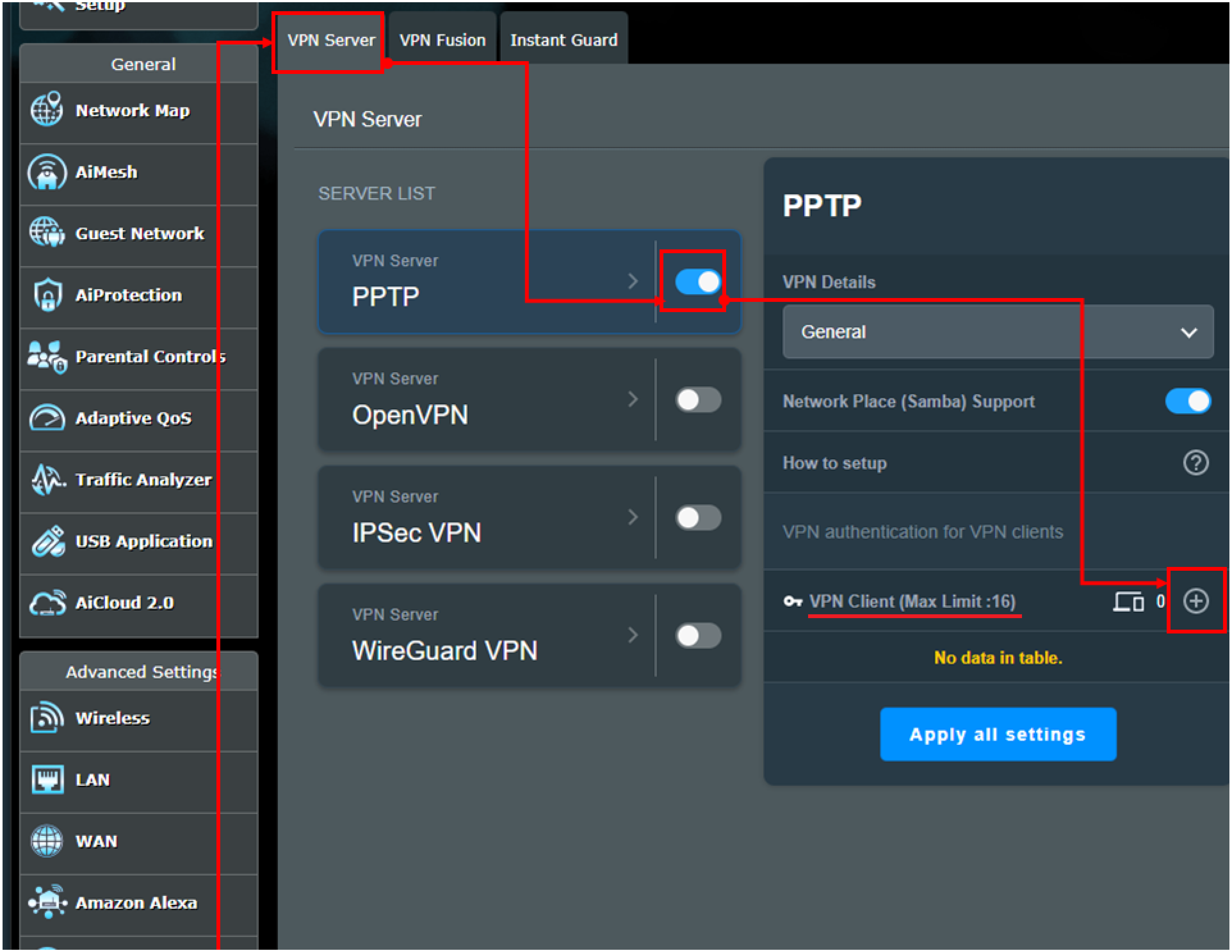
2. Key in your router's username and password to log in.



Note: If you forget the user name and/or password, please restore the router to the factory default status and setup.

Please refer to [Wireless Router] How to reset the router to factory default setting? for how to restore t to default status.

3. Click [VPN] > [VPN Server] > [PPTP] > Click □→■ [ON] icon in the VPN Server PPTP section to enable the f (default is OFF) > [VPN Client (Max Limit: 16)] Click "+" to add an account.

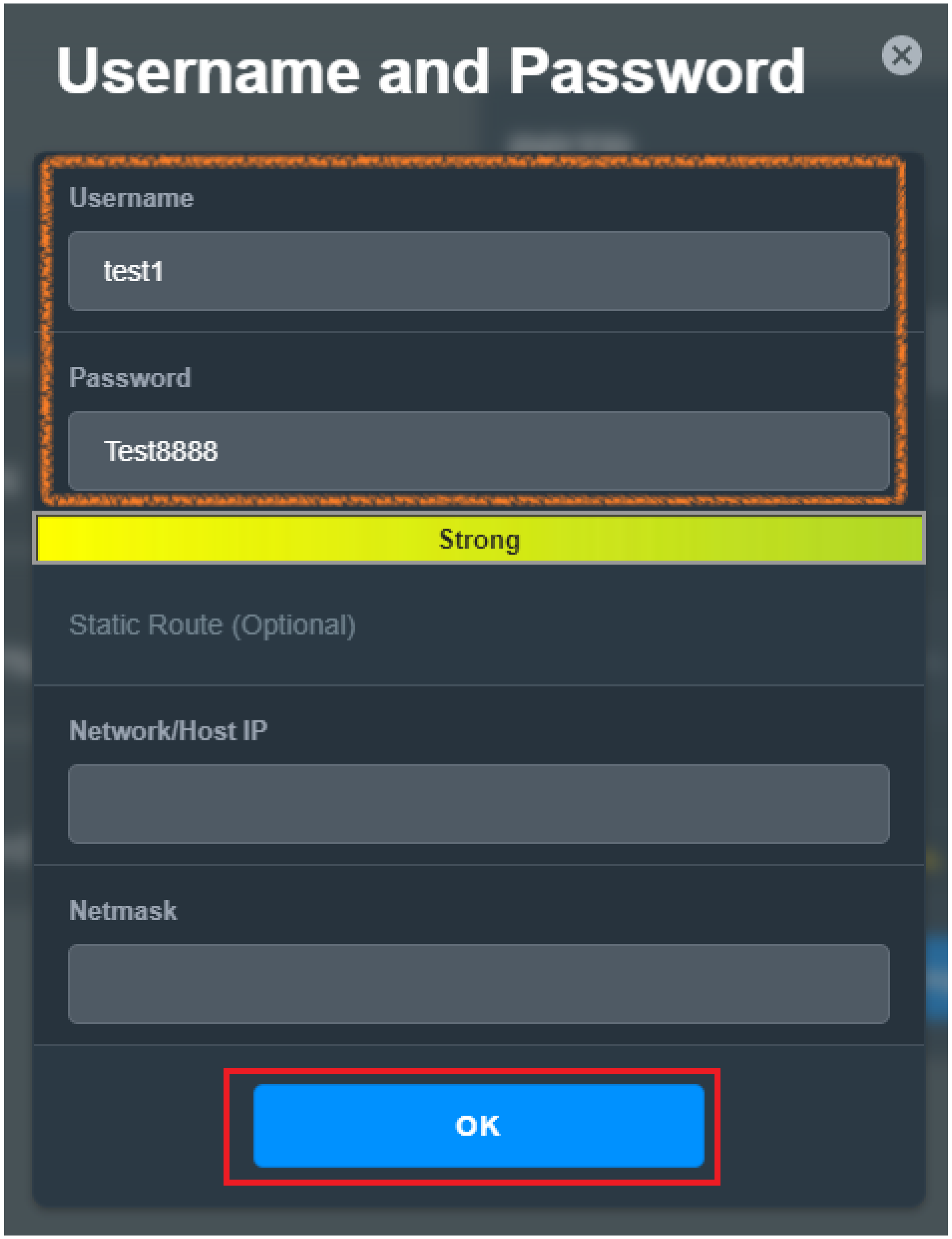

Setup
General
Network Map
AiMesh
Guest Network
AiProtection
Parental Controls
Adaptive QoS
Traffic Analyzer
USB Application
AiCloud 2.0
Advanced Settings
Wireless
LAN
WAN
Amazon Alexa
VPN Server
VPN Fusion
Instant Guard
VPN Server
SERVER LIST
VPN Server
PPTP
VPN Server
OpenVPN
VPN Server
IPSec VPN
VPN Server
WireGuard VPN
PPTP
VPN Details
General
Network Place (Samba) Support
How to setup
VPN authentication for VPN clients
VPN Client (Max Limit :16)
0
No data in table.
Apply all settings

4. Enter your custom [**Username**] and [**Password**] and click [OK]. Reminder: Once the [Username] and [Passw set, they cannot be modified.

Note: [Network/Host IP] and [Network Mask] under Static Route (Optional) are not mandatory and can be left

(1) Network/Host IP: Enter the IP address or network segment of the VPN client device (e.g., router).

(2) Network mask: It is recommended to enter 255.255.255.0.

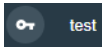


Username and Password

Username: test1

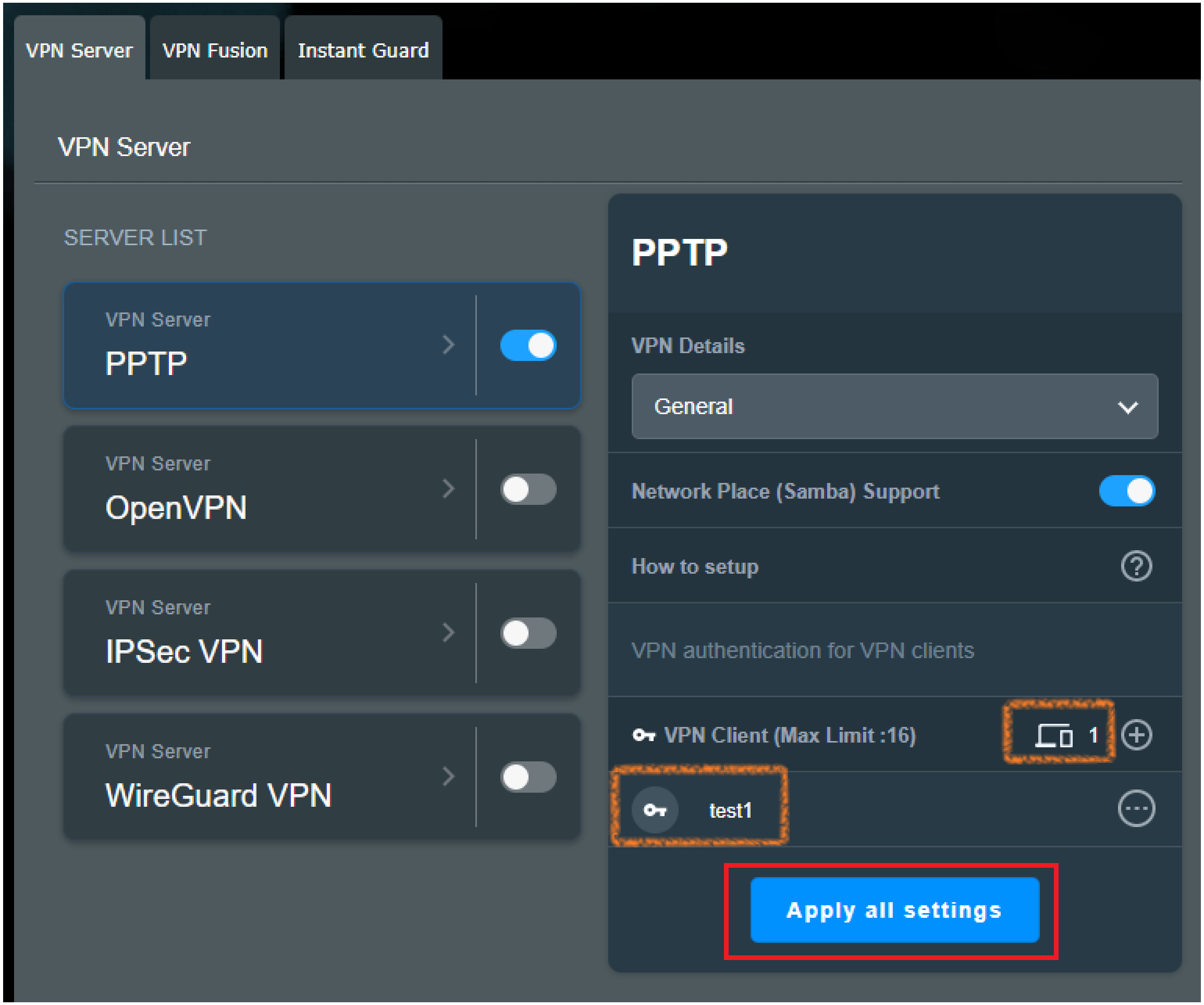
Password: Test8888

5. In the bottom right corner, the VPN client will display the number of newly added accounts, as shown in the fi showing 1 group of accounts 1

The VPN client will show the newly added username, as shown in the figure 

test

Finally, click [Apply all settings] to complete the settings on the router.



6. If you need advanced settings after completing the PPTP VPN server settings, click [**Advanced Settings**] in Detailed Settings dropdown menu.

The option settings shown in the figure below are all default items. After modifying the settings, click [**Apply a**
current settings] to complete the settings on the router.

Broadcast Support: Enabled by default.

Authentication: The default is [Auto], options include [MS-CHAPv1], [MS-CHAPv2].

MPPE Encryption: You can refer to the **VPN Client encryption setting table** to set.

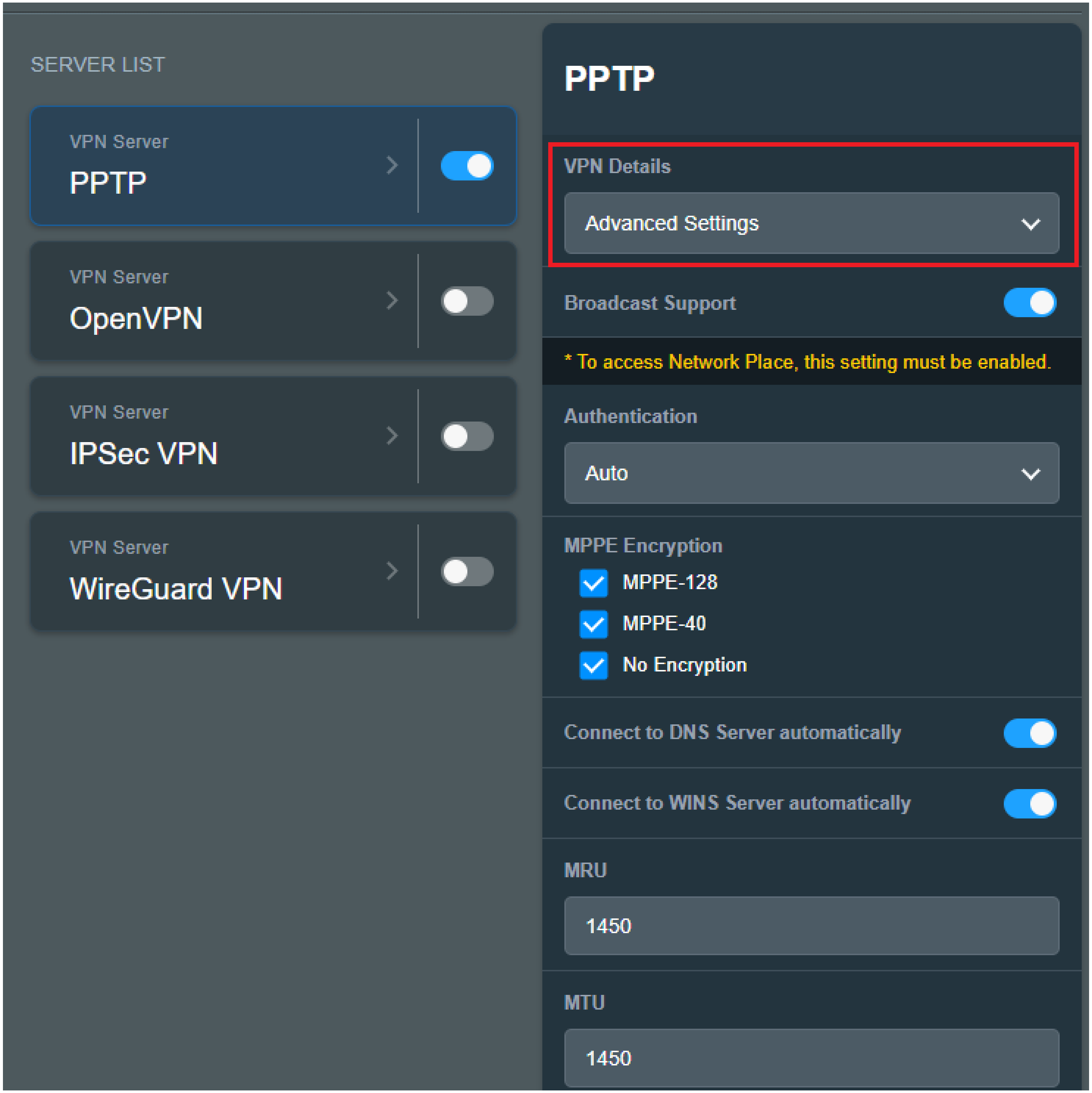
Connect to DNS Server automatically: Enabled by default.

Connect to WINS Server automatically: Enabled by default.

MRU: Maximum Receive Unit for data packets, default value is 1450.

MTU: Maximum Transmission Unit for data packets, default value is 1450.

Client IP address: Up to a maximum of 10 client IP addresses can be allocated, default range is 192.168.1



SERVER LIST

VPN Server PPTP ●

VPN Server OpenVPN ○

VPN Server IPSec VPN ○

VPN Server WireGuard VPN ○

PPTP

VPN Details: Advanced Settings

Broadcast Support ●

* To access Network Place, this setting must be enabled.

Authentication: Auto

MPPE Encryption

☑ MPPE-128

☑ MPPE-40

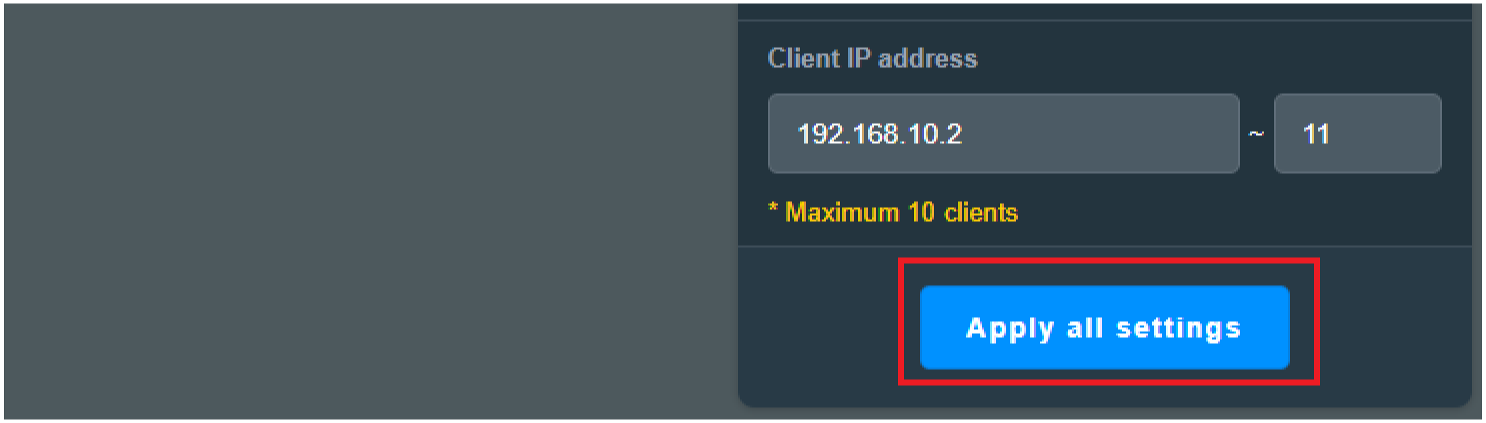
☑ No Encryption

Connect to DNS Server automatically ●

Connect to WINS Server automatically ●

MRU: 1450

MTU: 1450



Client IP address

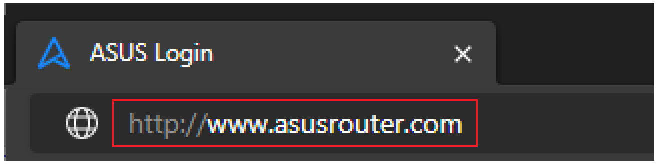
192.168.10.2 ~ 11

* Maximum 10 clients

Interface 2

Please follow the steps below to set up a VPN server - PPTP on your ASUS router.

1. Connect your computer to the router via wired or WiFi connection and enter **your router LAN IP** or router URL http://www.asusrouter.com to the WEB GUI.



http://www.asusrouter.com

Note: Please refer to How to enter the router setting page(Web GUI) to learn more.

2. Key in your router's username and password to log in.

Note: If you forget the user name and/or password, please restore the router to the factory default status and

Please refer to [Wireless Router] How to reset the router to factory default setting? for how to restore t

to default status.

3. Go to **VPN**

(1) Click "**VPN**”

(2) Click the lable of “**VPN Sever**”

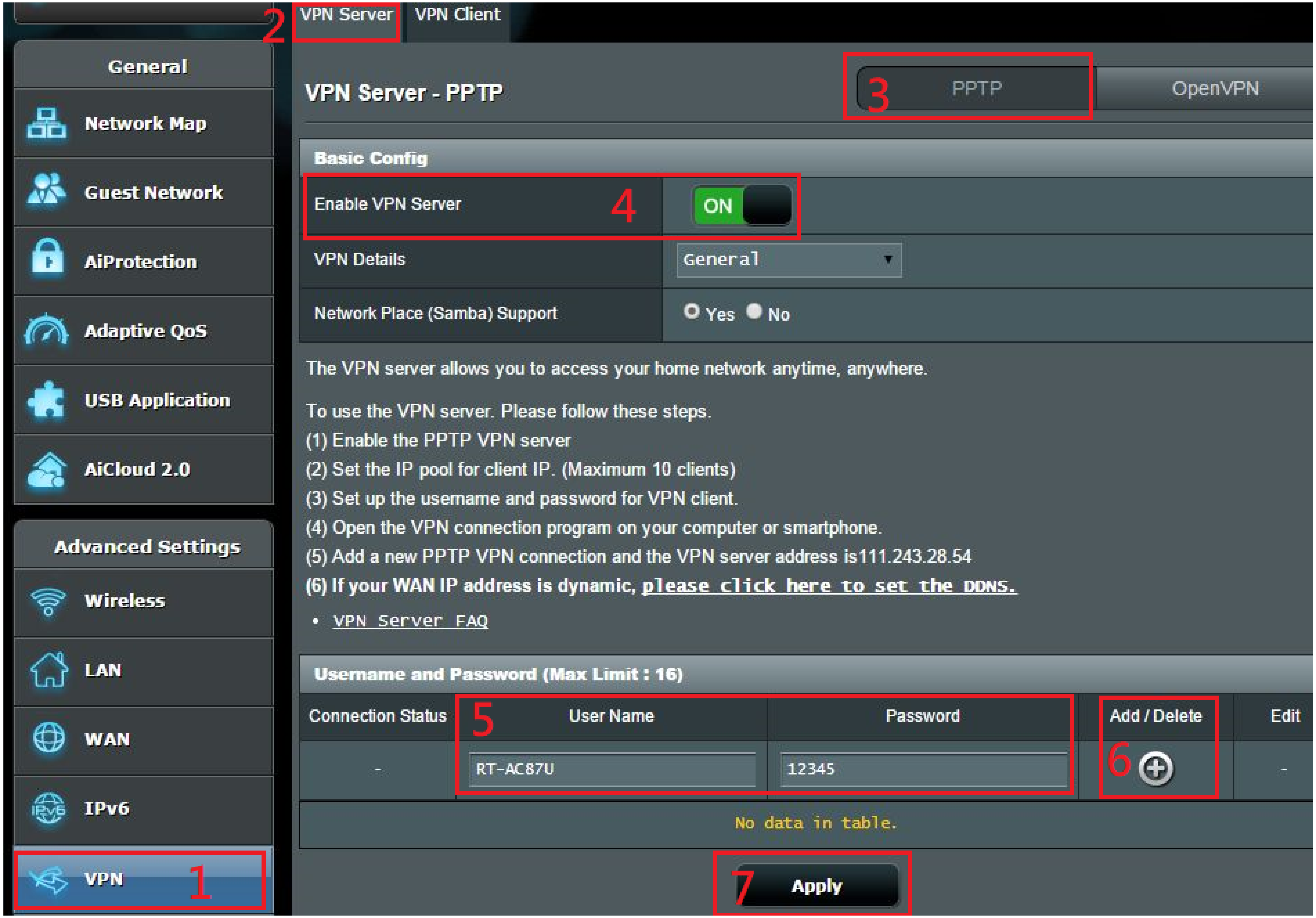
(3) Here select [**PPTP**] as VPN Server type.

(4) Click “**ON**” in item—“Enable VPN Sever”

(5) Enter “**User Name**” and “**Password**”

(6) Click “**+**”

(7) Click “**Apply**”to save.



VPN Server - PPTP

Basic Config

Enable VPN Server	ON
VPN Details	General
Network Place (Samba) Support	○ Yes ● No

The VPN server allows you to access your home network anytime, anywhere.

To use the VPN server. Please follow these steps.
(1) Enable the PPTP VPN server
(2) Set the IP pool for client IP. (Maximum 10 clients)
(3) Set up the username and password for VPN client.
(4) Open the VPN connection program on your computer or smartphone.
(5) Add a new PPTP VPN connection and the VPN server address is111.243.28.54
(6) If your WAN IP address is dynamic, please click here to set the DDNS.

- VPN Server FAQ

Username and Password (Max Limit : 16)

Connection Status	User Name	Password	Add / Delete	Edit
-	RT-AC87U	12345	⊕	-

No data in table.

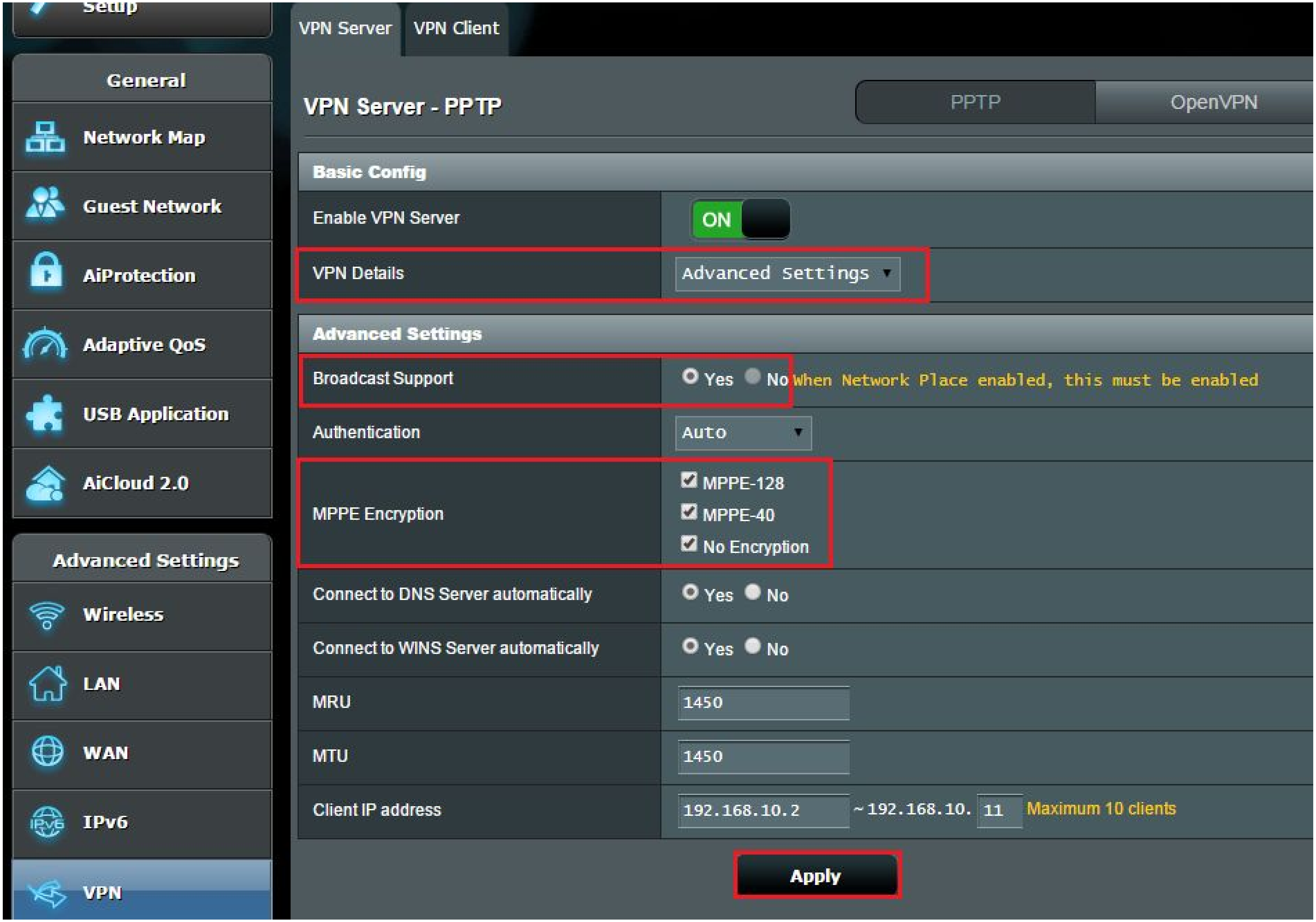
4. Advanced Settings

(1) If you want to do advanced settings for VPN Server, please select "**VPN Details**"

(2) Select “**Yes**” in item—“**Broadcast Support**”(When Network Place enable, this option must be enable.)

(3) Choose “**MEPPE Encryption**”, we will recommend to select all the options.

(4) Click button—“**Apply"**



VPN Server - PPTP

Basic Config

Enable VPN Server: ON

VPN Details: Advanced Settings

Advanced Settings

Broadcast Support: ○ Yes ● No When Network Place enabled, this must be enabled

Authentication: Auto

MPPE Encryption: ☑ MPPE-128 ☑ MPPE-40 ☑ No Encryption

Connect to DNS Server automatically: ○ Yes ● No

Connect to WINS Server automatically: ○ Yes ● No

MRU: 1450

MTU: 1450

Client IP address: 192.168.10.2 ~ 192.168.10. 11 Maximum 10 clients

Note 1: If your ISP is providing a Dynamic IP address to your network, your WAN IP address may change even applying the settings. Configure the **ASUS DDNS setting** to set up a fixed domain name.

Note 2: The Broadcast Support setting in **3-(2)** allows broadcast packet transfers between VPN clients and loca

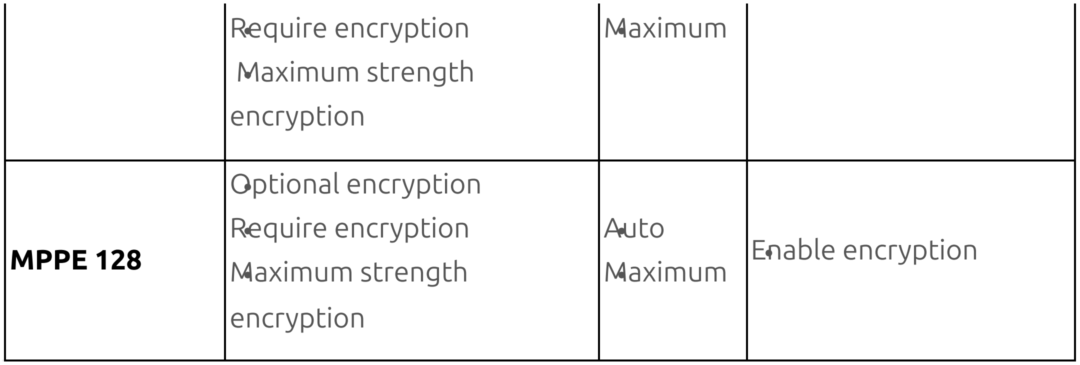
For example, the PC needs to send the broadcast packets to all LAN PCs to know which PC enables th Network Place Service.

The VPN client cannot send broadcast packets to the LAN while the Broadcast Support setting is disab

When Broadcast Support is disabled, VPN clients cannot detect the PC running Windows Network Plac will not be able to locate other PCs in the network. To connect to PCs in the LAN, VPN clients will manually hav the IP address to connect to a PC in the LAN.

Note 3: In Step **3-(3)**, administrators can set up VPN MPPE encryption settings and VPN client encryption settin based on the table below:

		VPN Client encryption setting **(VPN connection -> Properties -> Security -> Data encryption)**		
		Windows	**iOS, OS X**	**Android**
ASUS router VPN encryption setting **(Force MPPE Encryption)**	**Auto**	No encryption allowed Optional encryption Require encryption Maximum strength encryption	None	Disable encryption
	No encryption	No encryption allowed Optional encryption	None	Disable encryption
	MPPE 40	Optional encryption	Auto	Enable encryption

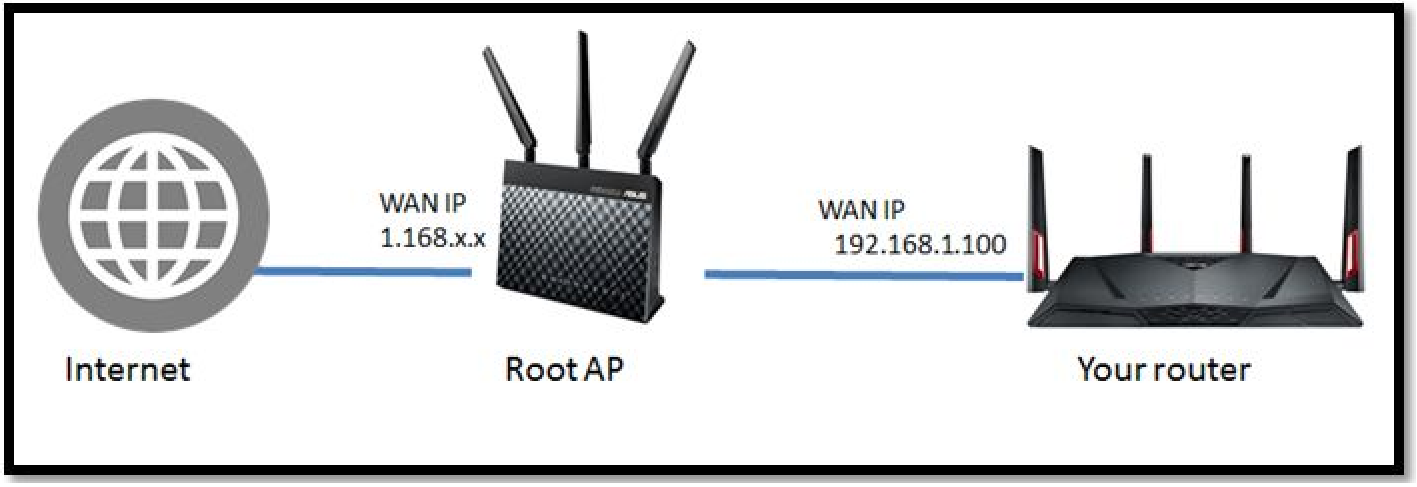


	Require encryption Maximum strength encryption	Maximum	
MPPE 128	Optional encryption Require encryption Maximum strength encryption	Auto Maximum	Enable encryption

FAQ

1. Can I connect to my home router from the external network using VPN if it has a private WAN IP addr as 192.168.x.x, 10.x.x.x, or 172.16.x.x?

When your router WAN IP is a private/virtual IP, it means that your router may be in the connection environme shown in the figure below, and there is another router in front that assigns an IP address to your router. In this c must set up port forwarding on another router's virtual server page in order to use VPN to connect back to your router from a remote external network. Please refer to the instructions on How to set up VPN server with port forwarding?



Note: To use VPN Server on your ASUS router, your router needs to have a public IP(WAN IP) from your ISP's service. This will allow devices on the internet to locate your ASUS router via a public IP(WAN IP).

If you are not sure of your public IP type, please check your Internet Service Provider (ISP).

2. Can the router use the private IP to set up the remote connection function?

Please note that if the router is using a private WAN IP address (such as connected behind another router/switch/modem with built-in router/Wi-Fi feature), could potentially place the router under a multi-layer NA network. This feature will not function properly under such environment.

Private IPv4 network ranges:

Class A: 10.0.0.0 – 10.255.255.255

Class B: 172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0 – 192.168.255.255

CGNAT IP network ranges:

The allocated address block is 100.64.0.0/10, i.e. IP addresses from 100.64.0.0 to 100.127.255.255.

How to get the (Utility / Firmware)?

You can download the latest drivers, software, firmware and user manuals in the **ASUS Download Center**.

If you need more information about the **ASUS Download Center**, please refer this **link**.

Was this information helpful?

YES NO

Contact Support

Please contact with us if the above information cannot resolve your problem

Get the support

- Above information might be partly or entirely quoted from exterior websites or sources. please refer to the information based on the source that we noted. Please directly contact or inquire the sources if there is any further question and note that ASUS is neither relevant nor responsible for its content/service
- This information may not suitable for all the products from the same category/series. Some of the screen shots and operations could be different from the software versions.
- ASUS provides the above information for reference only. If you have any questions about the content, please contact the above product vendor directly. Please note that ASUS is not responsible for the content or service provided by the above product vendor.
- Brand and product names mentioned are trademarks of their respective companies.

ASUS Support

Product Line	Inquiry service	Support service	Contact Us
Laptops	Warranty check	Product Registration	Call Us
Phone	Check repair status	ASUS Support Videos	Email Us
Motherboards	Find Service Locations		MyASUS
Tower PCs			

Monitors

Networking

Show All Products

Customer’s request on personal data

Terms of Use Notice | Privacy Policy

Global / English

FAQ

[Wireless Router] DDNS introduction and set up

Last Update : 2023/11/23 11:42

SEND TO EMAIL | OPEN ON YOUR SMART PHONE

Related Topics

[ASUS DDNS] How to remove the registered ASUS DDNS hostname in the router?

[Specification] How to check if the ASUS router supports the DDNS feature?

[Wireless Router] How to set up ASUS wireless router to access WebGUI/Router App from WAN?

[Wireless Router] How to bind trust account to my ASUS router?

[ASUS DDNS] How to transfer ASUS DDNS to new device ?

[Wireless Router] DDNS introduction and set up

What is DDNS?

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

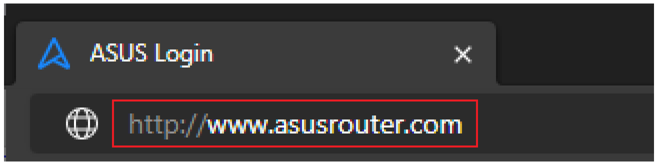
Prepare

1) The DDNS supported by ASUS routers vary by model, and it is recommended that you refer to ASUS product specifications to confirm that your router is supported. In this article, the ASUS router ZenWiFi AX is used as an example, and the settings screen may vary depending on the model and firmware version.

2) To use this feature on your ASUS router, your router needs to have a public IP(WAN IP) from your ISP's internet service. This will allow devices on the internet to locate your ASUS router via a public IP(WAN IP). If you are not sure of your public IP type, please check your Internet Service Provider (ISP).

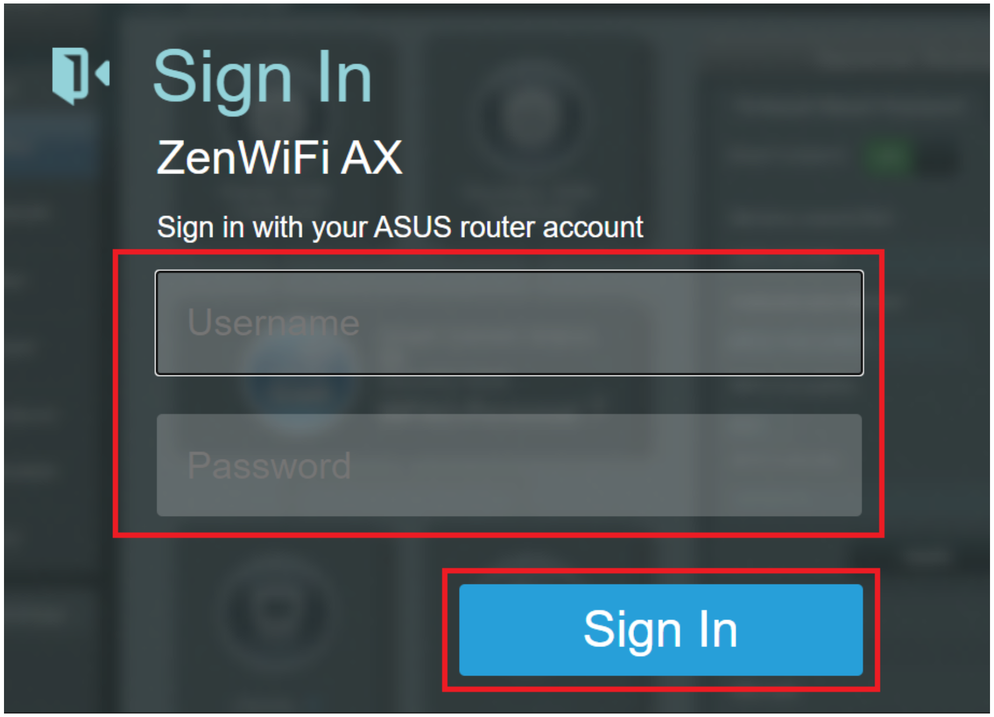
How to setup DDNS ?

Step 1. Connect your computer to the router via wired or WiFi connection and enter **your router LAN IP** or router URL http://www.asusrouter.com to the WEB GUI.



Please refer to How to enter the router setting page(Web GUI) to learn more.

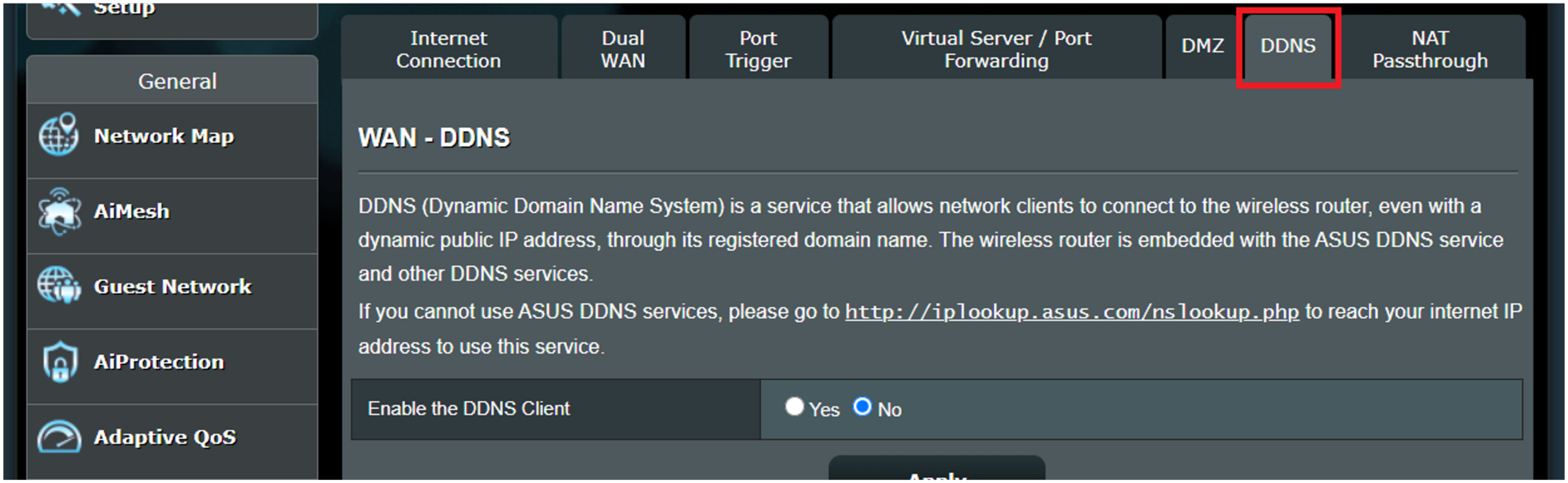
Step 2. Key in your router's username and password to log in.



Note: If you forget the user name and/or password, please restore the router to the factory default status and setup.

Please refer to How to reset the router to factory default setting for how to restore the router to default status.

Step 3. Go to **WAN**> **DDNS**



WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

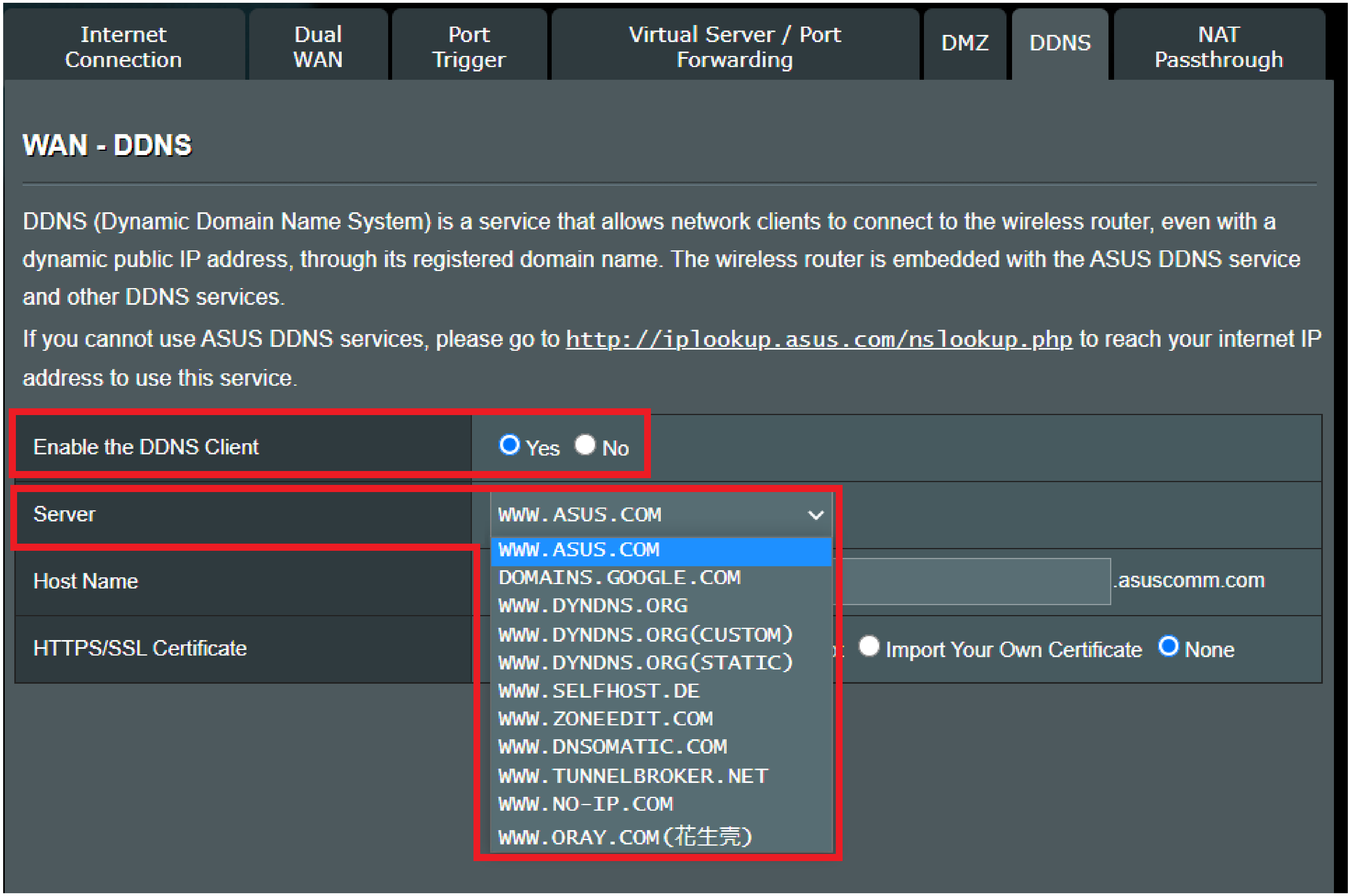
If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

Enable the DDNS Client ○ Yes ● No

Step 4. Enable the DDNS client, and then you can choose ASUS DDNS server [WWW.ASUS.COM] as server, which is totally free. There are also other DDNS servers for you to choose from.

Note: (1) The list of DDNS servers may vary depending on the firmware version or model differences.

Note:(2) If the wireless router is using a private WAN IP address (192.168.x.x, 10.x.x.x, 172.16.x.x or CGNAT IP, refer to FAQ5), this router may be under a multi-layer NAT network. The DDNS service is not able to work under this environment.



WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

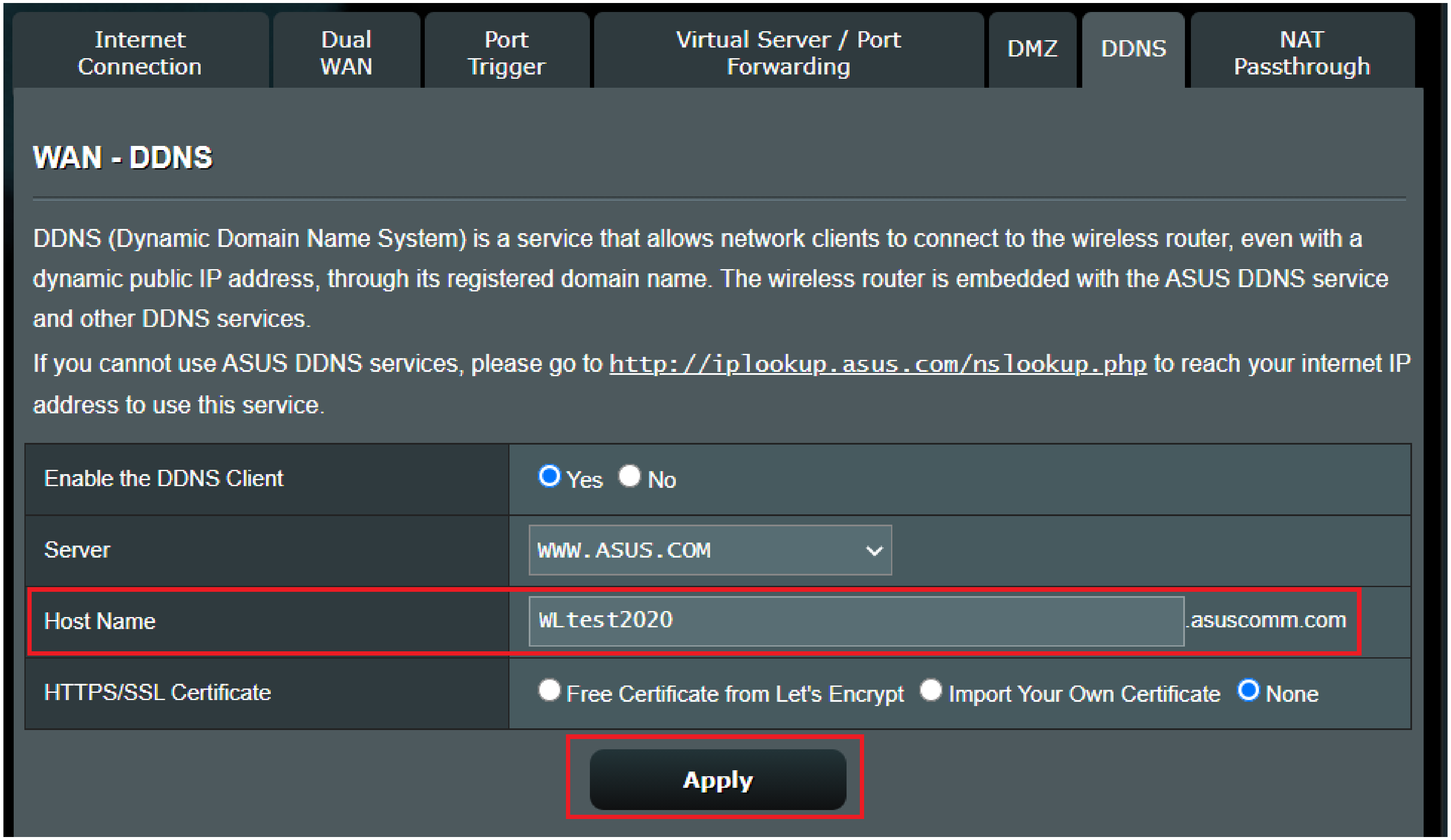
If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

Enable the DDNS Client	● Yes ○ No
Server	WWW.ASUS.COM
Host Name	.asuscomm.com
HTTPS/SSL Certificate	○ Import Your Own Certificate ● None

Step 5. The following is an example of using ASUS DDNS. Under **Host Name**, you can configure your own domain name. If the domain name has already been registered, please change to another one.

NOTE:

- The host name cannot accept number prefix and [.](such as [123abc]or [aaa.bbb]).
- If the domain name was registered by you but you want to use the previous domain name on the new ASUS router that you just purchased, please contact the ASUS Service Center.
- DDNS cannot be deleted if the router has the DDNS feature enabled and is in use.
- In the [host name] bar, you can change the domain name by clicking [**Apply**] after entering the name.
- After completing the configuration, click **[Apply]** to save.



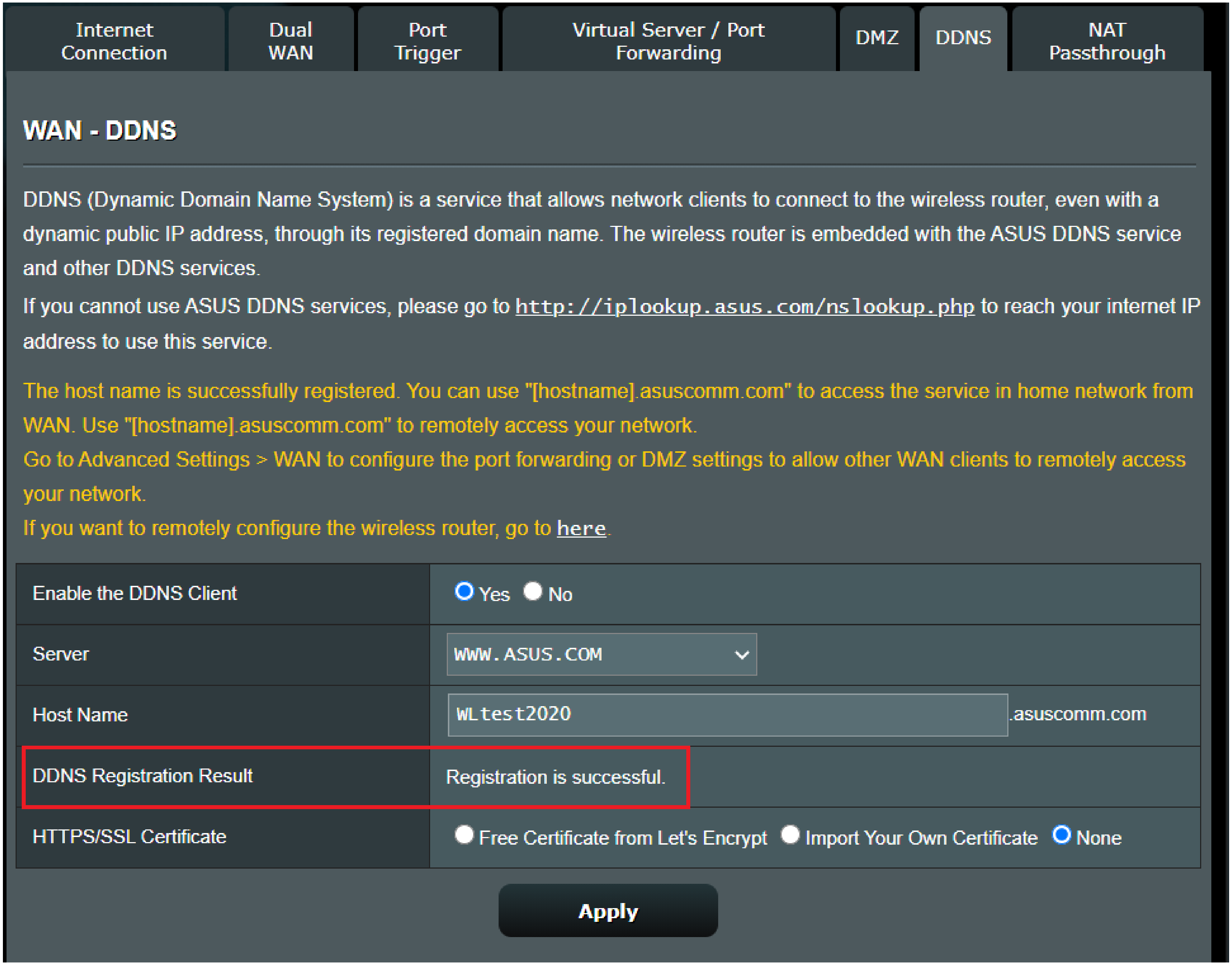
WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

Enable the DDNS Client	● Yes ○ No
Server	WWW.ASUS.COM
Host Name	WLtest2020 .asuscomm.com
HTTPS/SSL Certificate	○ Free Certificate from Let's Encrypt ○ Import Your Own Certificate ● None

Step 6. Registration is successful.



WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

The host name is successfully registered. You can use "[hostname].asuscomm.com" to access the service in home network from WAN. Use "[hostname].asuscomm.com" to remotely access your network.
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.
If you want to remotely configure the wireless router, go to here.

Enable the DDNS Client	● Yes ○ No
Server	WWW.ASUS.COM
Host Name	WLtest2020 .asuscomm.com
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	○ Free Certificate from Let's Encrypt ○ Import Your Own Certificate ● None

Check [**Network Map**] >> **[Internet status:**] >>DDNS name

Note: After upgrading the firmware to version 3.0.0.4.386.46061 or later, the router supports IPv6. For instruction about how to update the firmware.

Please refer to the support article : [Wireless Router] How to update the firmware of your router to the latest version ? (WebGUI)

If you want to transfer or delete the ASUS DDNS hostname, Please refer to FAQ

[ASUS DDNS] How do I remove the registered ASUS DDNS host name from my previous router?

[Wireless Router] How to transfer ASUS DDNS to new device?

FAQ

1. I would like to change the IP address of my router on the asuscomm.com service.

- The DDNS name is bound with the MAC address of the ASUS router.
- If you changed the ISP but the wan IP still is a public IP, then you still could use the same DDNS name.

2. Does ASUS router support customizing other DDNS services?

No, ASUS Router only support the DDNS services which was listed in the DDNS page now. The list of DDNS servers may vary depending on the firmware version or model differences.

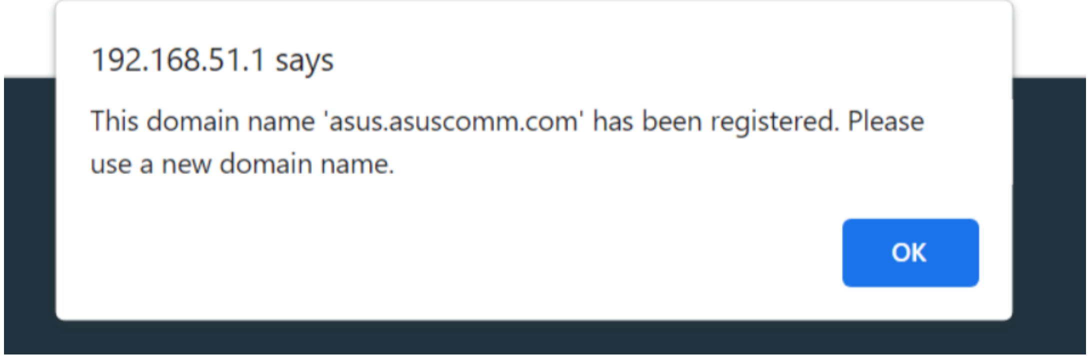
3. Why can't I use DDNS to access my home router from the outside network?

1. Registration of the DDNS service was not successful.
2. Check that the URL and port are correct. For more settings, please refer to [Wireless Router] How to set up ASUS wireless router to access WebGUI/Router App from WAN

4. Registration of the DDNS service was not successful.

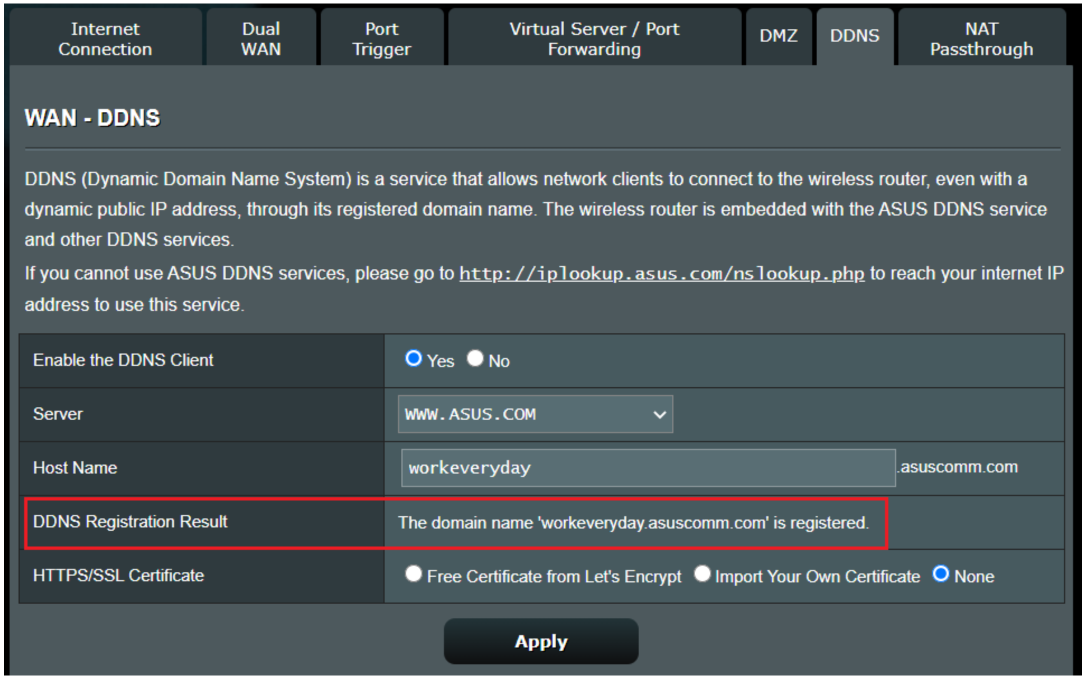
(1)The domain name [xxxxxxxx.asuscomm.com] is registered.

Please try using a different name.



192.168.51.1 says

This domain name 'asus.asuscomm.com' has been registered. Please use a new domain name.



WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

Enable the DDNS Client	● Yes ○ No
Server	WWW.ASUS.COM
Host Name	workeveryday .asuscomm.com
DDNS Registration Result	The domain name 'workeveryday.asuscomm.com' is registered.
HTTPS/SSL Certificate	○ Free Certificate from Let's Encrypt ○ Import Your Own Certificate ● None

(2) Invalid IP address

If the wireless router is using a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x), this router may be under a multi-layer NAT network. The DDNS service is not able to work under this environment.

5. Can the router use the private IP to set up the remote connection function?

Please note that if the router is using a private WAN IP address (such as connected behind another router/switch/modem with built-in router/WiFi feature), could potentially place the router under a multi-layer NAT network. This feature will not function properly under such environment.

Private IPv4 network ranges:

Class A: 10.0.0.0 – 10.255.255.255

Class B: 172.16.0.0 – 172.31.255.255

Class C: 192.168.0.0 – 192.168.255.255

CGNAT IP network ranges:

The allocated address block is 100.64.0.0/10, i.e. IP addresses from 100.64.0.0 to 100.127.255.255.

How to get the (Utility / Firmware)?

You can download the latest drivers, software, firmware and user manuals in the ASUS Download Center.

If you need more information about the **ASUS Download Center**, please refer this link.

Was this information helpful?

YES NO

Contact Support

Please contact with us if the above information cannot resolve your problem

Get the support

- Above information might be partly or entirely quoted from exterior websites or sources. please refer to the information based on the source that we noted. Please directly contact or inquire the sources if there is any further question and note that ASUS is neither relevant nor responsible for its content/service
- This information may not suitable for all the products from the same category/series. Some of the screen shots and operations could be different from the software versions.
- ASUS provides the above information for reference only. If you have any questions about the content, please contact the above product vendor directly. Please note that ASUS is not responsible for the content or service provided by the above product vendor.
- Brand and product names mentioned are trademarks of their respective companies.

ASUS Support

Product Line
Laptops
Phone
Motherboards
Tower PCs
Monitors
Networking
Show All Products

Inquiry service
Warranty check
Check repair status
Find Service Locations

Support service
Product Registration
ASUS Support Videos

Contact Us
Call Us
Email Us
MyASUS
Customer’s request on personal data

Terms of Use Notice | Privacy Policy Global / English

FAQ

[Wireless Router] How to configure Router to use Pi-Hole?

Last Update : 2023/05/16 16:12

SEND TO EMAIL | OPEN ON YOUR SMART PHONE

[Wireless Router] How to configure Router to use Pi-Hole?

If you encounter Blocking ads fail while using Pi-Hole, you might try the following steps:

Note: If the device is connecting to the router using a VPN client, ads cannot be blocked.

Please refer to How to set up a DNS server on a VPN server in the router?

Before starting the setup, please check the firmware version of your router.

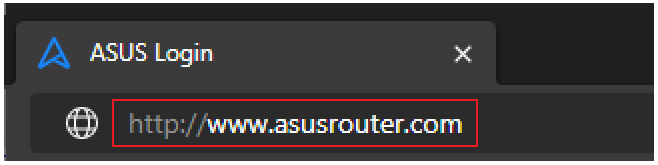
If your router firmware version >= 3.0.0.4.386.45898

Please assign the pi-hole IP in the WAN DNS setting.

Step1: Connect your PC to ASUS router via Wi-Fi or Ethernet cable.

Step2: Open a web browser and enter **your router LAN IP** or router URL http://www.asusrouter.com to the WEB GUI.

Key in your router's username and password to log in.



Note: Please refer to How to enter the router setting page(Web GUI) (ASUSWRT)? to learn more.

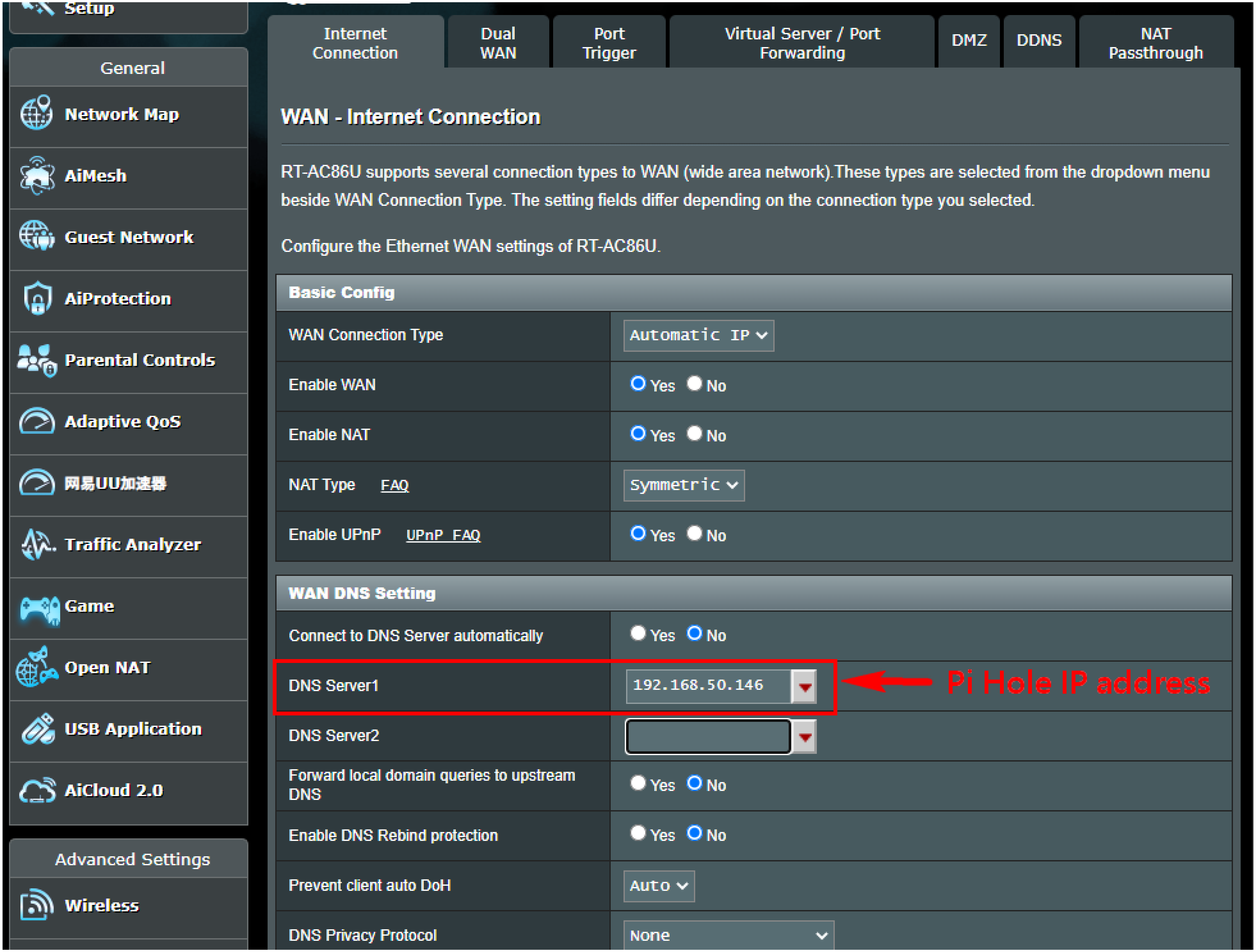
Note: If you forget the user name and/or password, please restore the router to the factory default status and setup.

Please refer to [Wireless Router] How to reset the router to factory default setting? for how to restore the router to default status.

Step3: Go to [**WAN**] > [**Internet Connection**] tab.

Step4: Set Connect to DNS Server automatically as [**No**]

Step5: Enter device IP address on DNS server and click [**Apply**] to save.



WAN - Internet Connection

RT-AC86U supports several connection types to WAN (wide area network).These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of RT-AC86U.

Basic Config	
WAN Connection Type	Automatic IP
Enable WAN	● Yes ○ No
Enable NAT	● Yes ○ No
NAT Type FAQ	Symmetric
Enable UPnP UPnP FAQ	● Yes ○ No

WAN DNS Setting	
Connect to DNS Server automatically	○ Yes ● No
DNS Server1	192.168.50.146
DNS Server2	
Forward local domain queries to upstream DNS	○ Yes ● No
Enable DNS Rebind protection	○ Yes ● No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

Pi Hole IP address

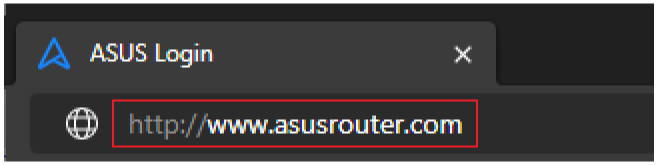
If your router firmware version < 3.0.0.4.386.45898

Please follow the steps to assign the pi-hole IP in LAN setting.

Step1: Connect your PC to ASUS router via Wi-Fi or Ethernet cable.

Step2: Open a web browser and enter **your router LAN IP** or router URL http://www.asusrouter.com to the WEB GUI.

Key in your router's username and password to log in.



Note: Please refer to How to enter the router setting page(Web GUI) (ASUSWRT)? to learn more.

Note: If you forget the user name and/or password, please restore the router to the factory default status and setup.

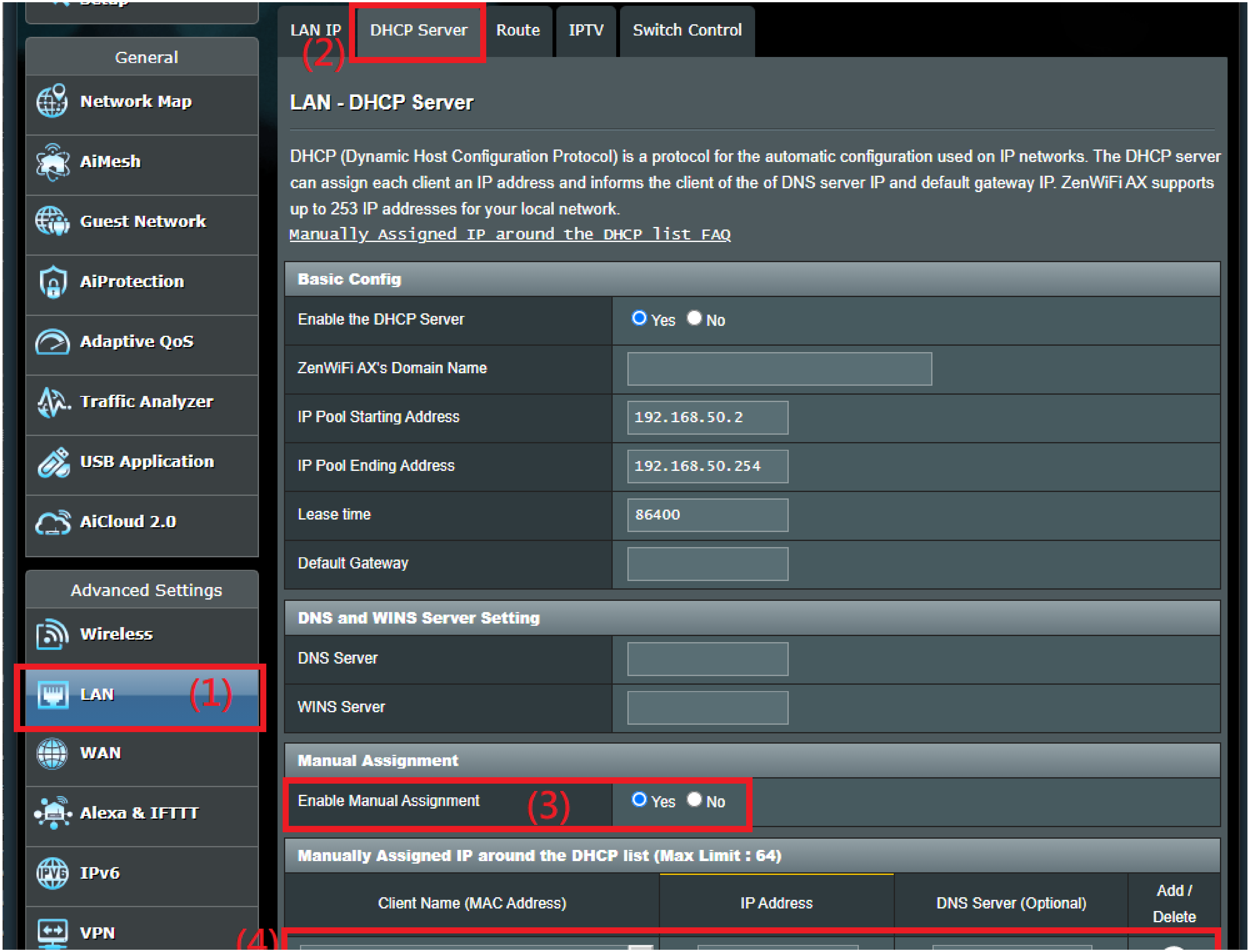
Please refer to [Wireless Router] How to reset the router to factory default setting? for how to restore the router to default status.

Step3: Go to [**LAN**] -> [**DHCP Server**] tab.

Step4: Enable [**Enable Manual Assignment**]

Step5: Choose Pi-Hole to configure on **Client name** and click Add/Delete button.

For information on how to check the IP address of the device, please refer to [Wireless Router] How to check for devices connected on ASUS router?



LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the of DNS server IP and default gateway IP. ZenWiFi AX supports up to 253 IP addresses for your local network.

Manually Assigned IP around the DHCP list FAQ

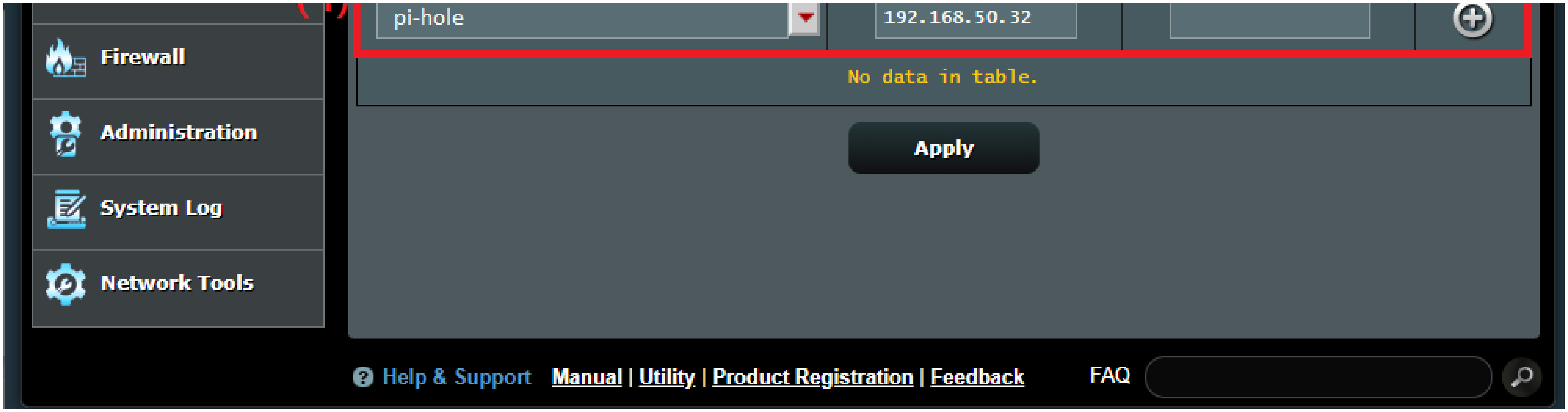
Basic Config	
Enable the DHCP Server	● Yes ○ No
ZenWiFi AX's Domain Name	
IP Pool Starting Address	192.168.50.2
IP Pool Ending Address	192.168.50.254
Lease time	86400
Default Gateway	

DNS and WINS Server Setting	
DNS Server	
WINS Server	

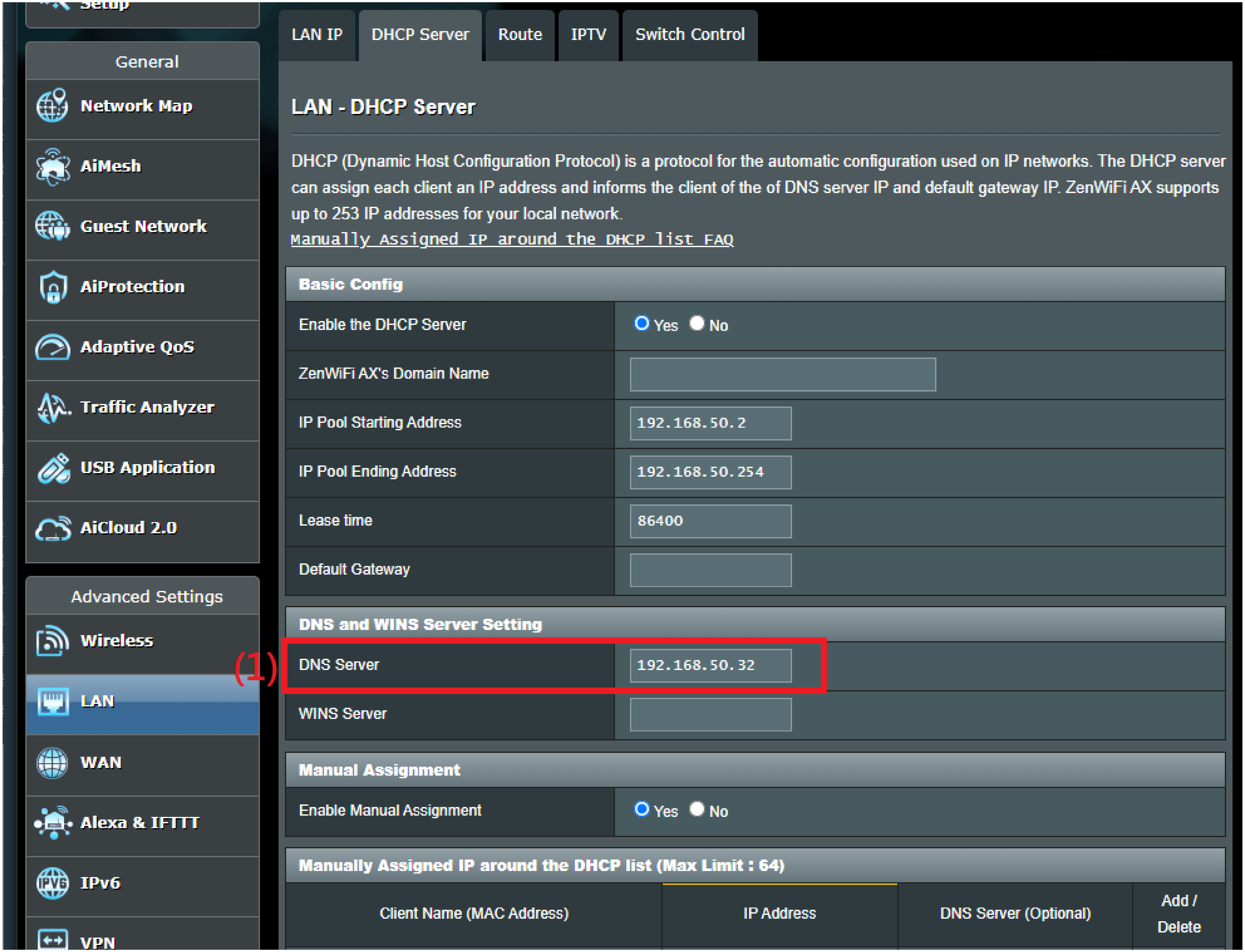
Manual Assignment	
Enable Manual Assignment	● Yes ○ No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Add / Delete



Step6: Enter Pi-Hole IP address on DNS server and click [**Apply**] to save.



LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the of DNS server IP and default gateway IP. ZenWiFi AX supports up to 253 IP addresses for your local network.

Manually Assigned IP around the DHCP list FAQ

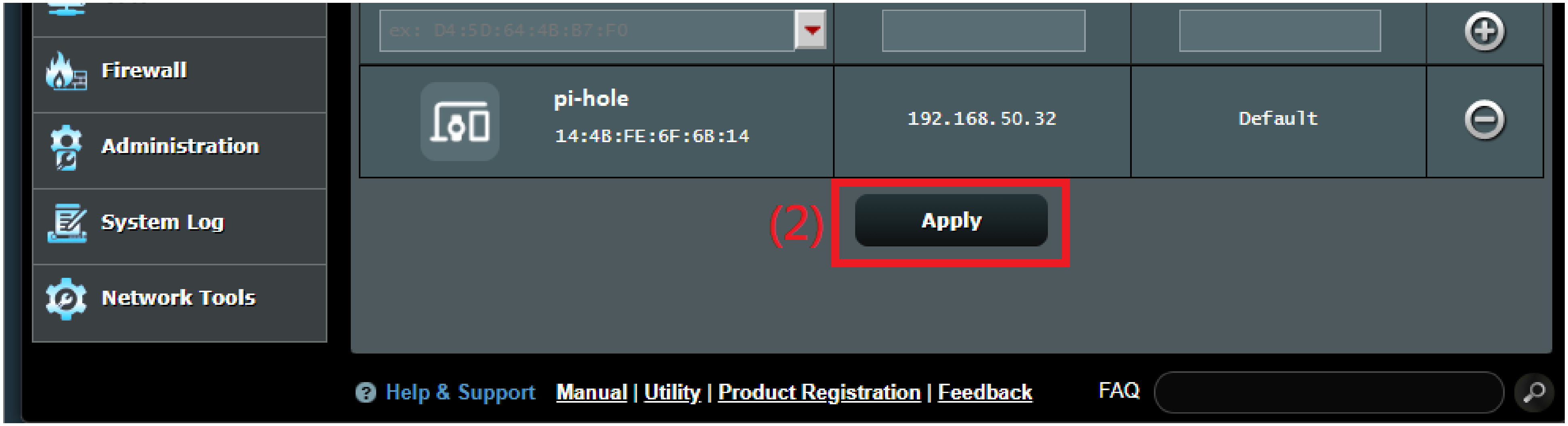
Basic Config	
Enable the DHCP Server	● Yes ○ No
ZenWiFi AX's Domain Name	
IP Pool Starting Address	192.168.50.2
IP Pool Ending Address	192.168.50.254
Lease time	86400
Default Gateway	

DNS and WINS Server Setting	
DNS Server	192.168.50.32
WINS Server	

Manual Assignment	
Enable Manual Assignment	● Yes ○ No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Add / Delete

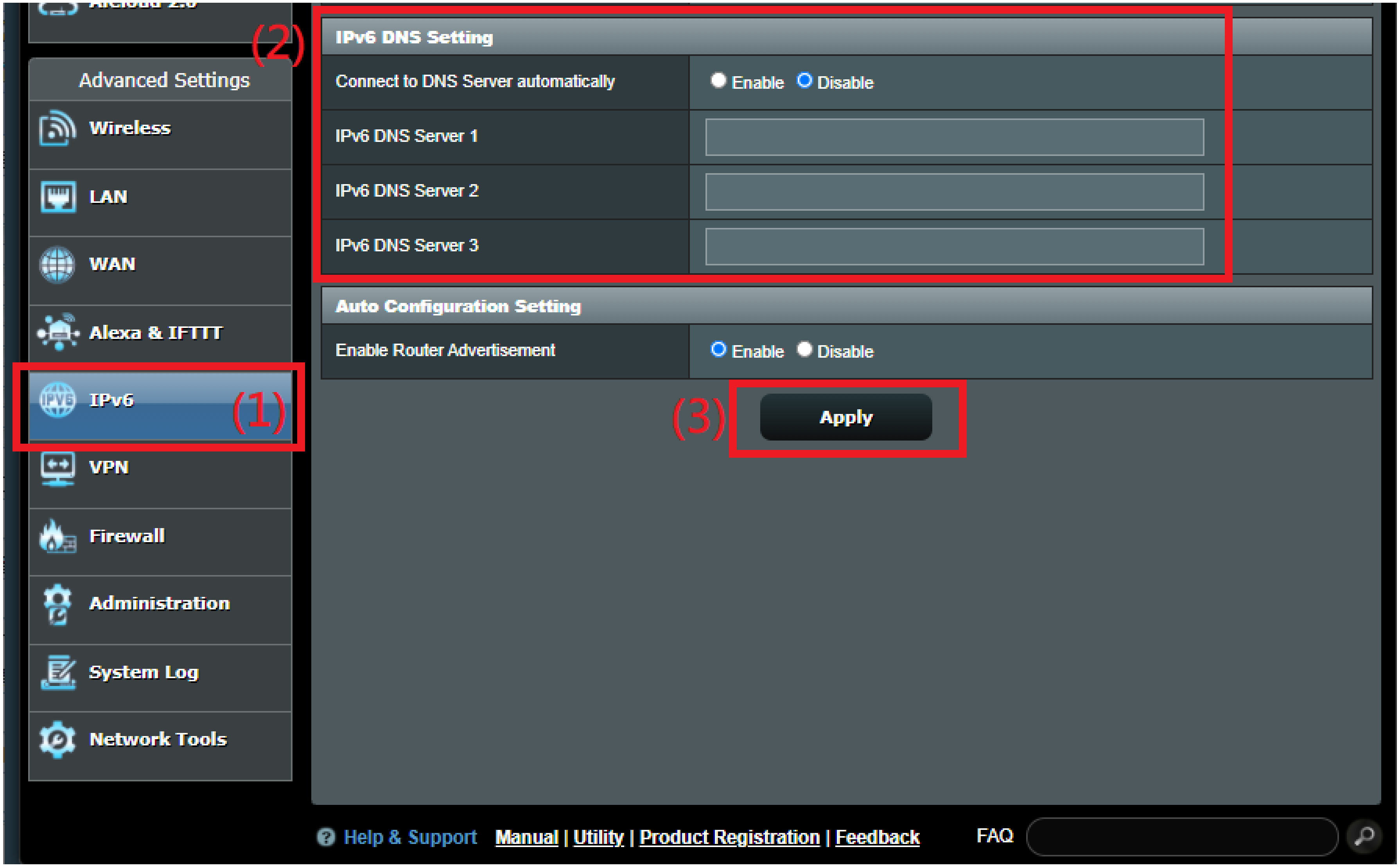


pi-hole 14:4B:FE:6F:6B:14	192.168.50.32	Default	⊖

FAQ

1. Pi-hole supports IPv6, how to set up IPv6 DNS Server?

- Go to [**IPv6**] -> [**IPv6 DNS Setting**], enter Pi-Hole IPv6 IP address on IPv6 DNS server and click [**Apply**] to save. General IPv6 setting information, please refer to [IPv6] How to set up IPv6 in ASUS Router?



IPv6 DNS Setting

Connect to DNS Server automatically	○ Enable ● Disable
IPv6 DNS Server 1	
IPv6 DNS Server 2	
IPv6 DNS Server 3	

Auto Configuration Setting

Enable Router Advertisement	● Enable ○ Disable

2. What's the difference of setting up Pi-hole DNS in WAN and in LAN of asus router?

It actually doens't matter for the asus routers. The functions are the same for the connected clients. The only thing needs to be checked is the Firmware Version of your router due to it will decide if the Pi-hole DNS server should be set in the LAN setting page or WAN setting page.

You could only find the difference in the Pi-hole console > logs. If you want to know more about that, please kindly contact to the provider of Pi-hole.

How to get the (Utility / Firmware)?

You can download the latest drivers, software, firmware and user manuals in the ASUS Download Center.

If you need more information about the **ASUS Download Center**, please refer to this link.

Was this information helpful?

YES NO

Contact Support

Please contact with us if the above information cannot resolve your problem

Get the support

- Above information might be partly or entirely quoted from exterior websites or sources. please refer to the information based on the source that we noted. Please directly contact or inquire the sources if there is any further question and note that ASUS is neither relevant nor responsible for its content/service
- This information may not suitable for all the products from the same category/series. Some of the screen shots and operations could be different from the software versions.
- ASUS provides the above information for reference only. If you have any questions about the content, please contact the above product vendor directly. Please note that ASUS is not responsible for the content or service provided by the above product vendor.
- Brand and product names mentioned are trademarks of their respective companies.

ASUS Support

Product Line

Laptops

Phone

Motherboards

Tower PCs

Monitors

Networking

Show All Products

Inquiry service

Warranty check

Check repair status

Find Service Locations

Support service

Product Registration

ASUS Support Videos

Contact Us

Call Us

Email Us

MyASUS

Customer’s request on personal data

Terms of Use Notice | Privacy Policy 🌐 Global / English

FAQ

[Wireless Router] How to set up a DNS server on a VPN server in the router?

SEND TO EMAIL | OPEN ON YOUR SMART PHONE

[Wireless Router] How to set up a DNS server on a VPN server in the router?

Note: The VPN feature does not support IPv6, ads cannot be blocked.

General VPN server setting information, please refer to

[VPN] How to set up a VPN server on ASUS router – PPTP

[VPN] How to set up a VPN server on ASUS router – OpenVPN

[VPN] How to set up a VPN server on ASUS router –IPSec VPN

Please check the IP address of the device before setting up, please refer to this [Wireless Router] How to check for devices connected on ASUS router?

1. PPTP VPN server

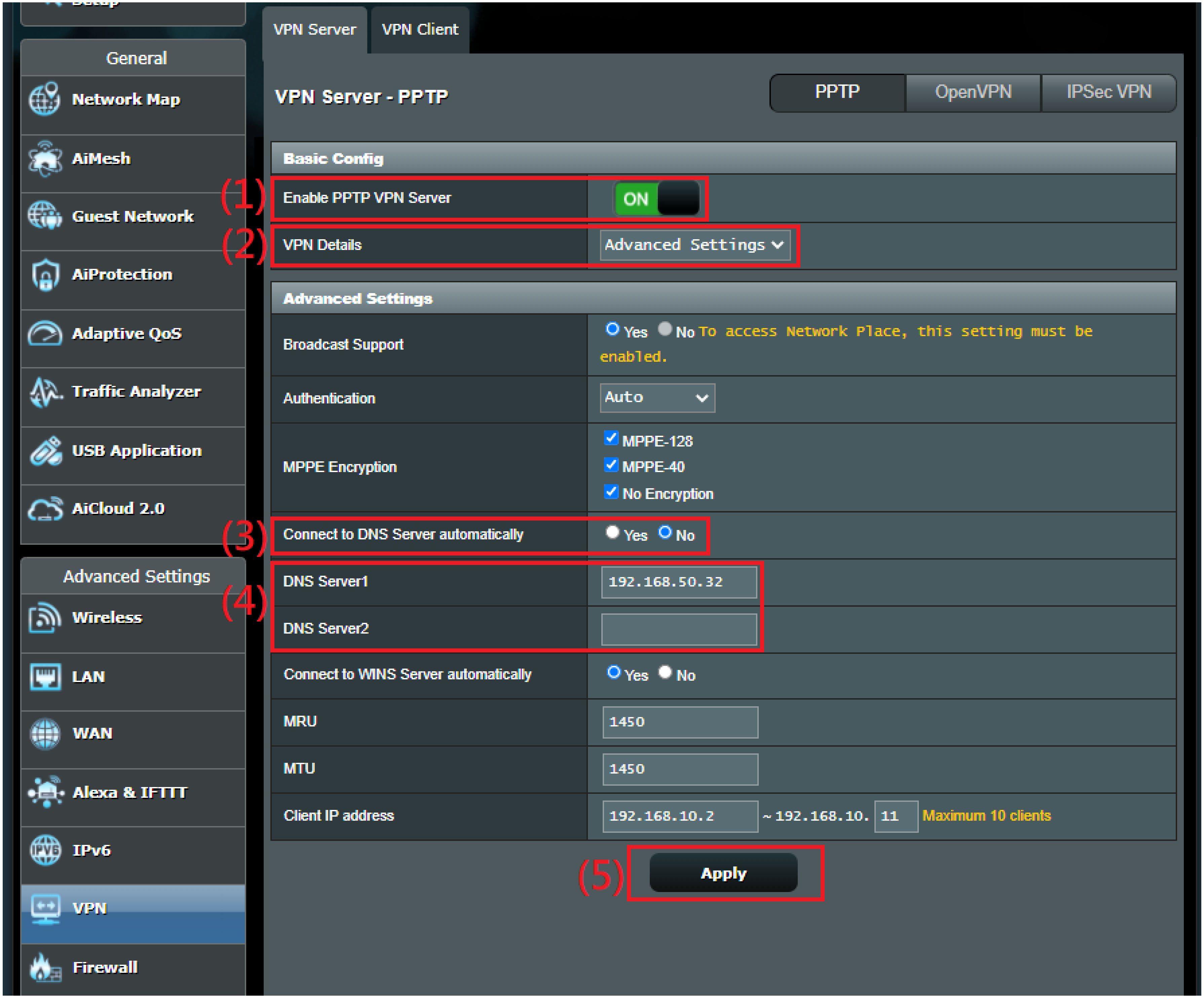
Step1: Enable PPTP VPN Server

Step2: Choose [**Advanced Settings] for VPN Details**

Step3: Set Connect to DNS Server automatically as [No]

Step4: Enter device IP address on DNS server.

Step5: Click [**Apply**] to save.



VPN Server - PPTP

Basic Config

(1) Enable PPTP VPN Server: ON

(2) VPN Details: Advanced Settings

Advanced Settings

Broadcast Support: ● Yes ○ No To access Network Place, this setting must be enabled.

Authentication: Auto

MPPE Encryption: ☑ MPPE-128 ☑ MPPE-40 ☑ No Encryption

(3) Connect to DNS Server automatically: ○ Yes ● No

(4) DNS Server1: 192.168.50.32

DNS Server2:

Connect to WINS Server automatically: ● Yes ○ No

MRU: 1450

MTU: 1450

Client IP address: 192.168.10.2 ~ 192.168.10. 11 Maximum 10 clients

(5) Apply

2. OpenVPN server

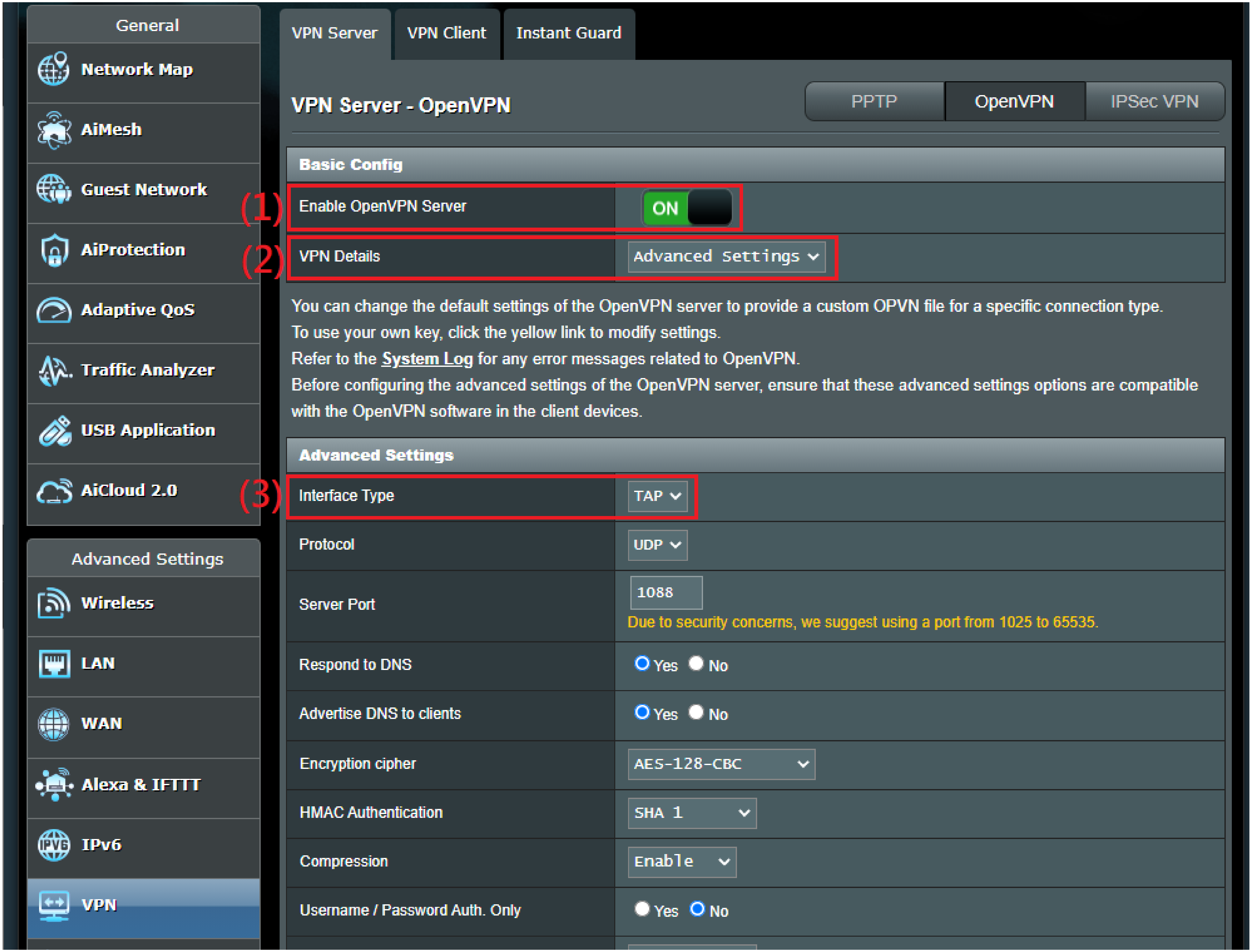
Step1: Enable OpenVPN Server

Step2: Choose [**Advanced Settings] for VPN Details**

Step3: Choose [**TAP] for Interface type**

Step4: Set Direct clients to redirect internet traffic as [Yes]

Step5: Click [**Apply**] to save.



VPN Server - OpenVPN

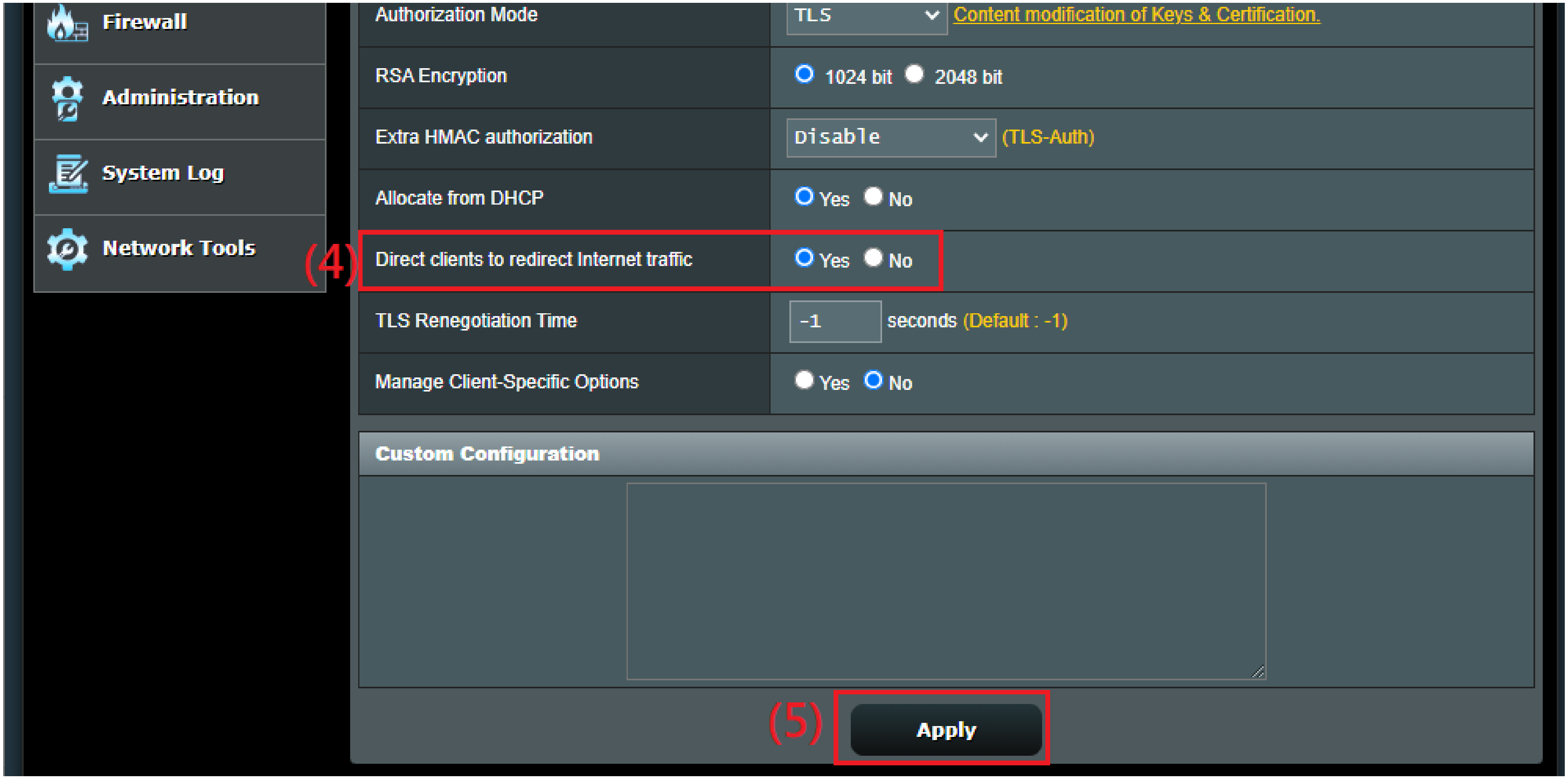
Basic Config

Enable OpenVPN Server	ON
VPN Details	Advanced Settings

You can change the default settings of the OpenVPN server to provide a custom OPVN file for a specific connection type.
To use your own key, click the yellow link to modify settings.
Refer to the System Log for any error messages related to OpenVPN.
Before configuring the advanced settings of the OpenVPN server, ensure that these advanced settings options are compatible with the OpenVPN software in the client devices.

Advanced Settings

Interface Type	TAP
Protocol	UDP
Server Port	1088 Due to security concerns, we suggest using a port from 1025 to 65535.
Respond to DNS	● Yes ○ No
Advertise DNS to clients	● Yes ○ No
Encryption cipher	AES-128-CBC
HMAC Authentication	SHA 1
Compression	Enable
Username / Password Auth. Only	○ Yes ● No



Authorization Mode	TLS Content modification of Keys & Certification.
RSA Encryption	● 1024 bit ○ 2048 bit
Extra HMAC authorization	Disable (TLS-Auth)
Allocate from DHCP	● Yes ○ No
Direct clients to redirect Internet traffic	● Yes ○ No
TLS Renegotiation Time	-1 seconds (Default : -1)
Manage Client-Specific Options	○ Yes ● No

Custom Configuration

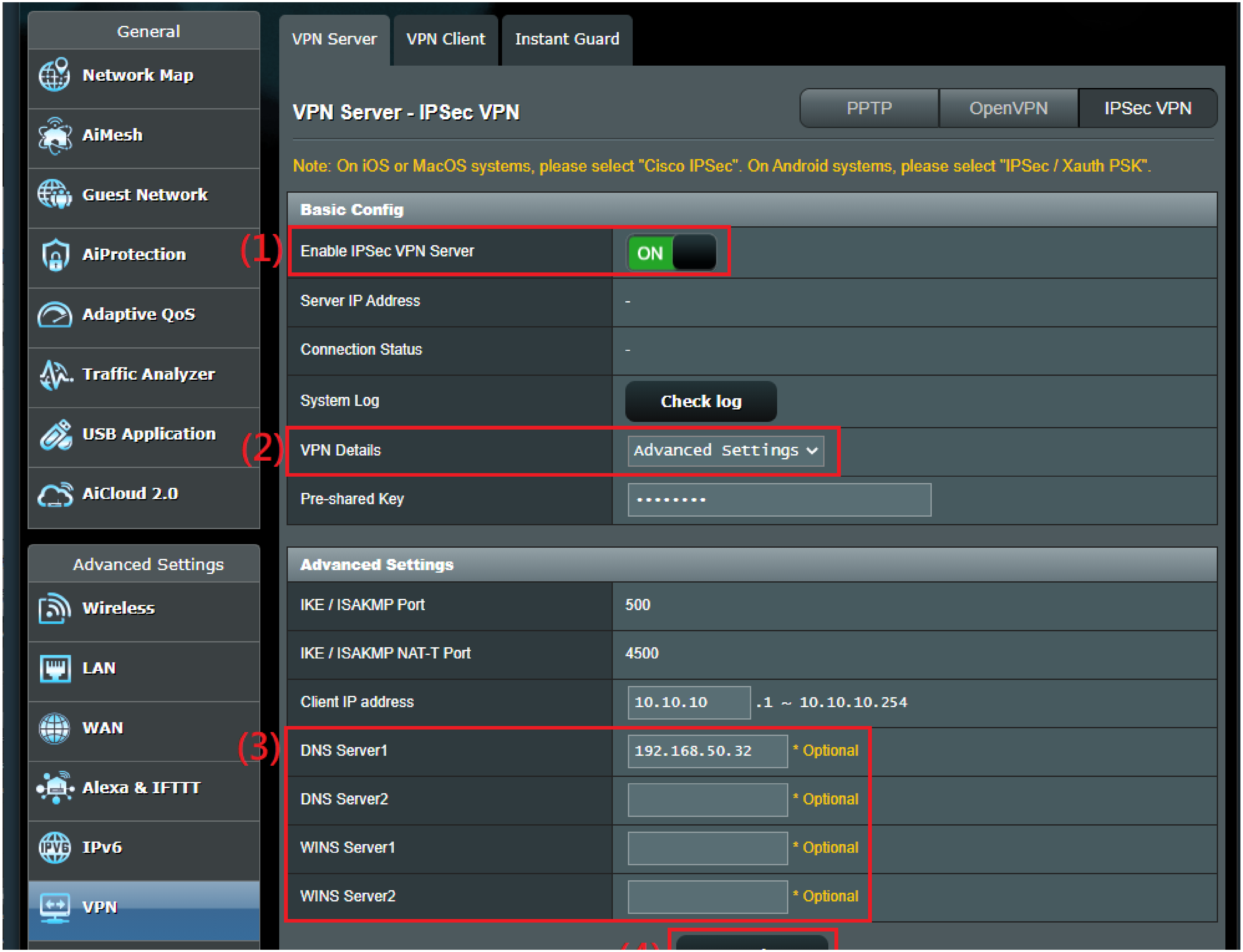
3. IPSec VPN server

Step1: Enable IPSec VPN Server

Step2: Choose [**Advanced Settings] for VPN Details**

Step3: Enter device IP address on DNS server.

Step4: Click [**Apply**] to save.



VPN Server - IPSec VPN

Note: On iOS or MacOS systems, please select "Cisco IPSec". On Android systems, please select "IPSec / Xauth PSK".

Basic Config	
Enable IPSec VPN Server	ON
Server IP Address	-
Connection Status	-
System Log	Check log
VPN Details	Advanced Settings
Pre-shared Key	••••••••

Advanced Settings	
IKE / ISAKMP Port	500
IKE / ISAKMP NAT-T Port	4500
Client IP address	10.10.10 .1 ~ 10.10.10.254
DNS Server1	192.168.50.32 * Optional
DNS Server2	* Optional
WINS Server1	* Optional
WINS Server2	* Optional

How to get the (Utility / Firmware)?

You can download the latest drivers, software, firmware and user manuals in the ASUS Download Center.

If you need more information about the **ASUS Download Center**, please refer this link.

Was this information helpful?

YES NO

Contact Support

Please contact with us if the above information cannot resolve your problem

Get the support

- Above information might be partly or entirely quoted from exterior websites or sources. please refer to the information based on the source that we noted. Please directly contact or inquire the sources if there is any further question and note that ASUS is neither relevant nor responsible for its content/service
- This information may not suitable for all the products from the same category/series. Some of the screen shots and operations could be different from the software versions.
- ASUS provides the above information for reference only. If you have any questions about the content, please contact the above product vendor directly. Please note that ASUS is not responsible for the content or service provided by the above product vendor.
- Brand and product names mentioned are trademarks of their respective companies.

Terms of Use Notice | Privacy Policy

Global / English

FAQ

[Wireless Router] How to set up Pi-hole® with ASUS NAS to block Ads?

Last Update : 2022/10/14 10:59

SEND TO EMAIL | OPEN ON YOUR SMART PHONE

[Wireless Router] How to set up Pi-hole® with ASUS NAS to block Ads?

Pi-hole® is an ad-blocking software and powerful local DNS service who helps to audit queried domains on your network.

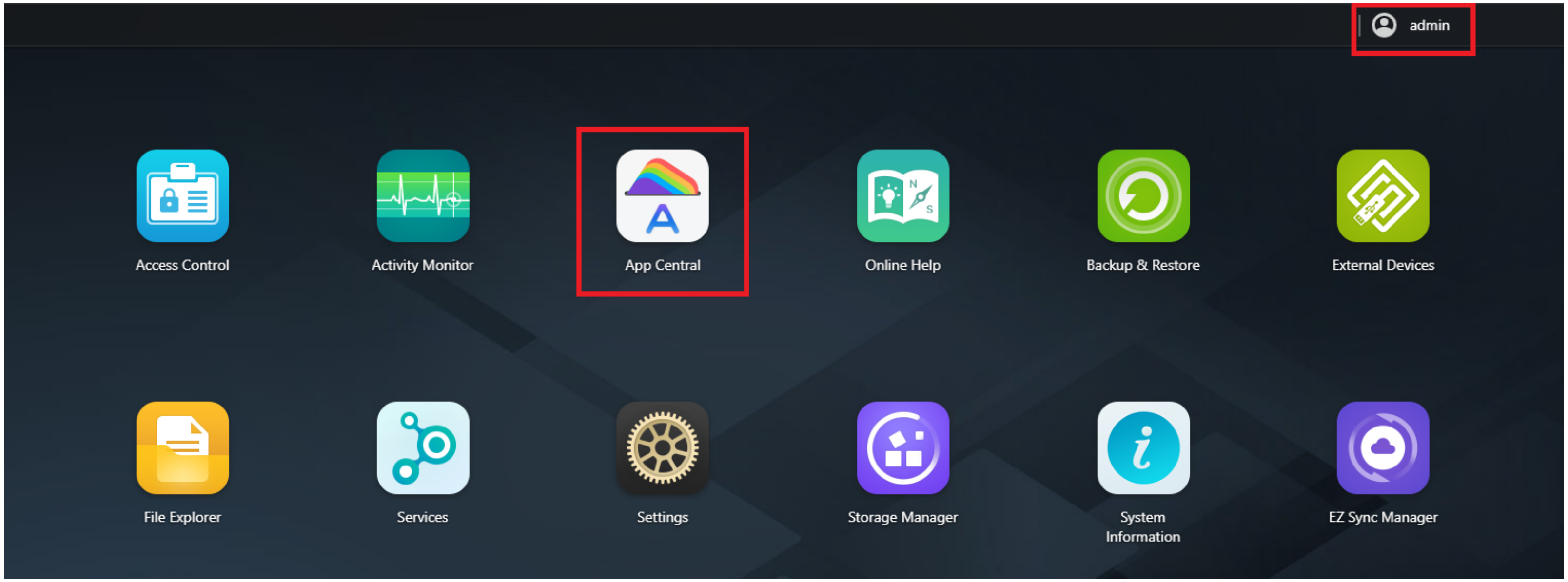
Pi-hole® can also operate in many systems, this article will show you how to easily install on NAS and configure DNS on router.

We take AS6602T as an example to build the system.

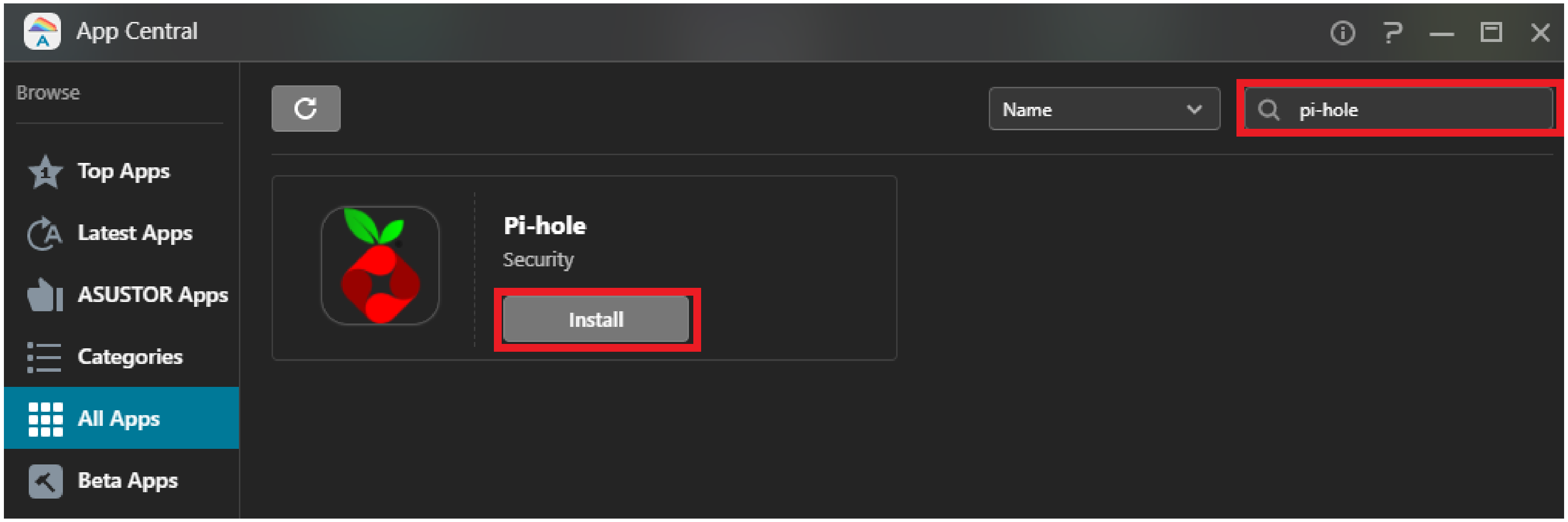
Notice: Please update your router firmware to the latest version, Pi-hole settings will differ by router firmware version. For more info, please refer to FAQ: [Wireless Router] How to configure Router to use Pi-Hole?

Step 1 Install Pi-hole in ASUSTOR App Central

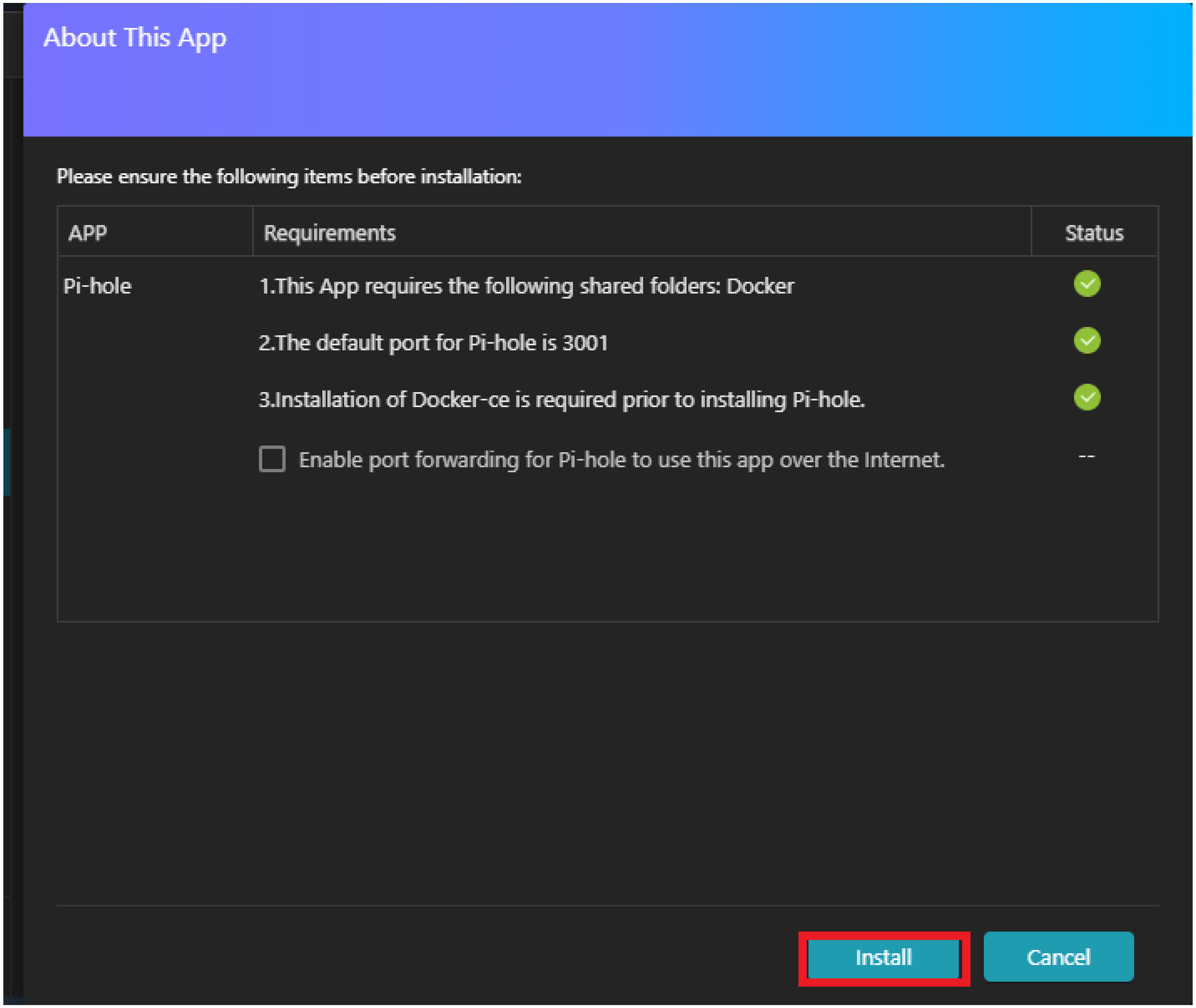
1-1 Log in to ADM and click [**App Central**].



1-2 Search "**Pi-hole"** and click [**Install**] button to install Pi-hole App.



1-3 Review “About This App” and click [**Install**].

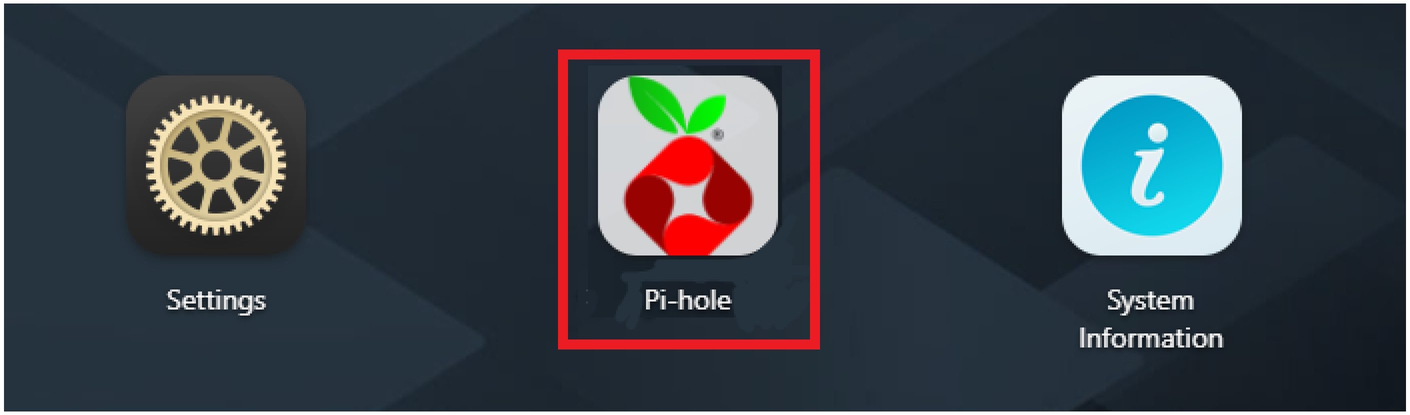


About This App

Please ensure the following items before installation:

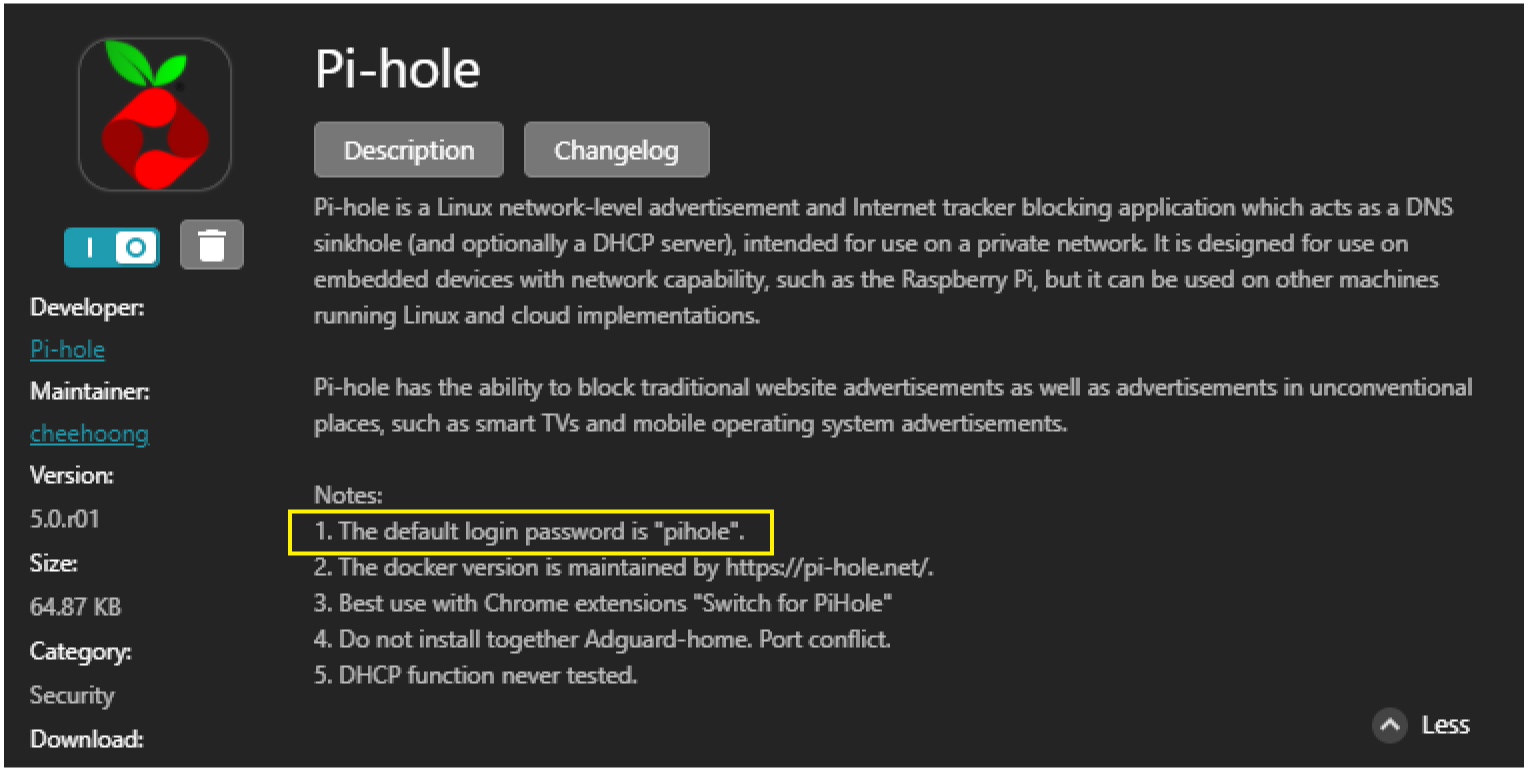
APP	Requirements	Status
Pi-hole	1.This App requires the following shared folders: Docker	✓
	2.The default port for Pi-hole is 3001	✓
	3.Installation of Docker-ce is required prior to installing Pi-hole.	✓
	□ Enable port forwarding for Pi-hole to use this app over the Internet.	--

Step 2 Check the result after installed. Return to NAS home page and click Pi-hole.



Notice: Pi-hole default login password is in Notes.

For more info of Pi-hole® related settings, please visit Pi-hole® website: https://pi-hole.net/



Pi-hole

Pi-hole is a Linux network-level advertisement and Internet tracker blocking application which acts as a DNS sinkhole (and optionally a DHCP server), intended for use on a private network. It is designed for use on embedded devices with network capability, such as the Raspberry Pi, but it can be used on other machines running Linux and cloud implementations.

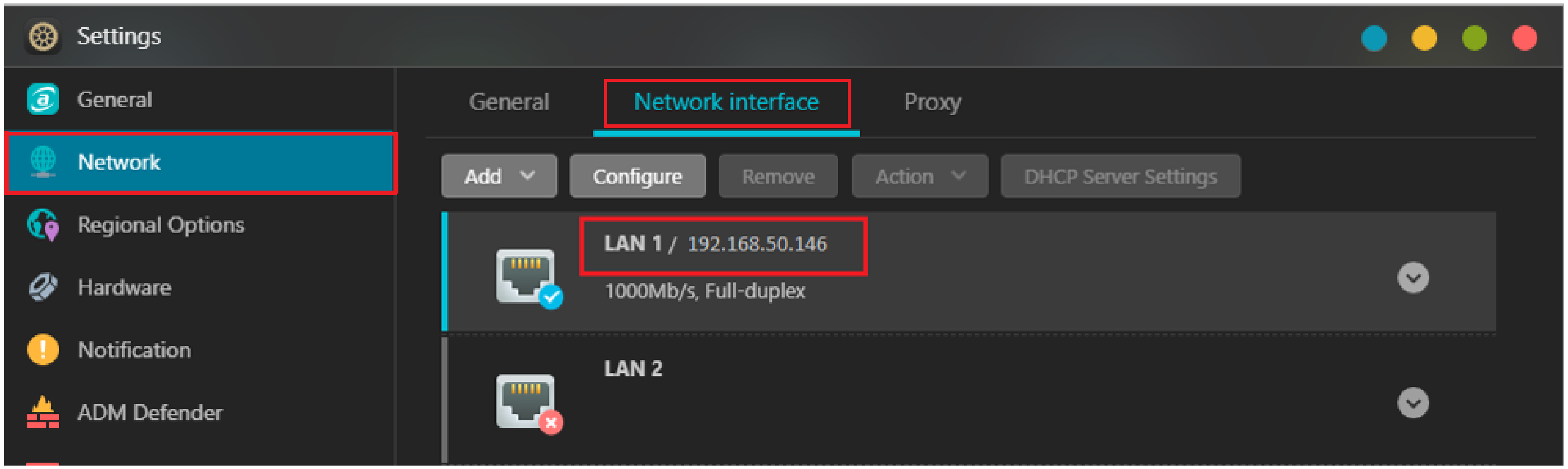
Pi-hole has the ability to block traditional website advertisements as well as advertisements in unconventional places, such as smart TVs and mobile operating system advertisements.

Notes:
1. The default login password is "pihole".
2. The docker version is maintained by https://pi-hole.net/.
3. Best use with Chrome extensions "Switch for PiHole"
4. Do not install together Adguard-home. Port conflict.
5. DHCP function never tested.

Developer:
Pi-hole
Maintainer:
cheehoong
Version:
5.0.r01
Size:
64.87 KB
Category:
Security
Download:

Step 3 Check NAS IP address

Select [**Settings**] -> [**Network**] -> [**Network Interface**] and then select LAN port depending on your connection.



LAN 1 / 192.168.50.146
1000Mb/s, Full-duplex

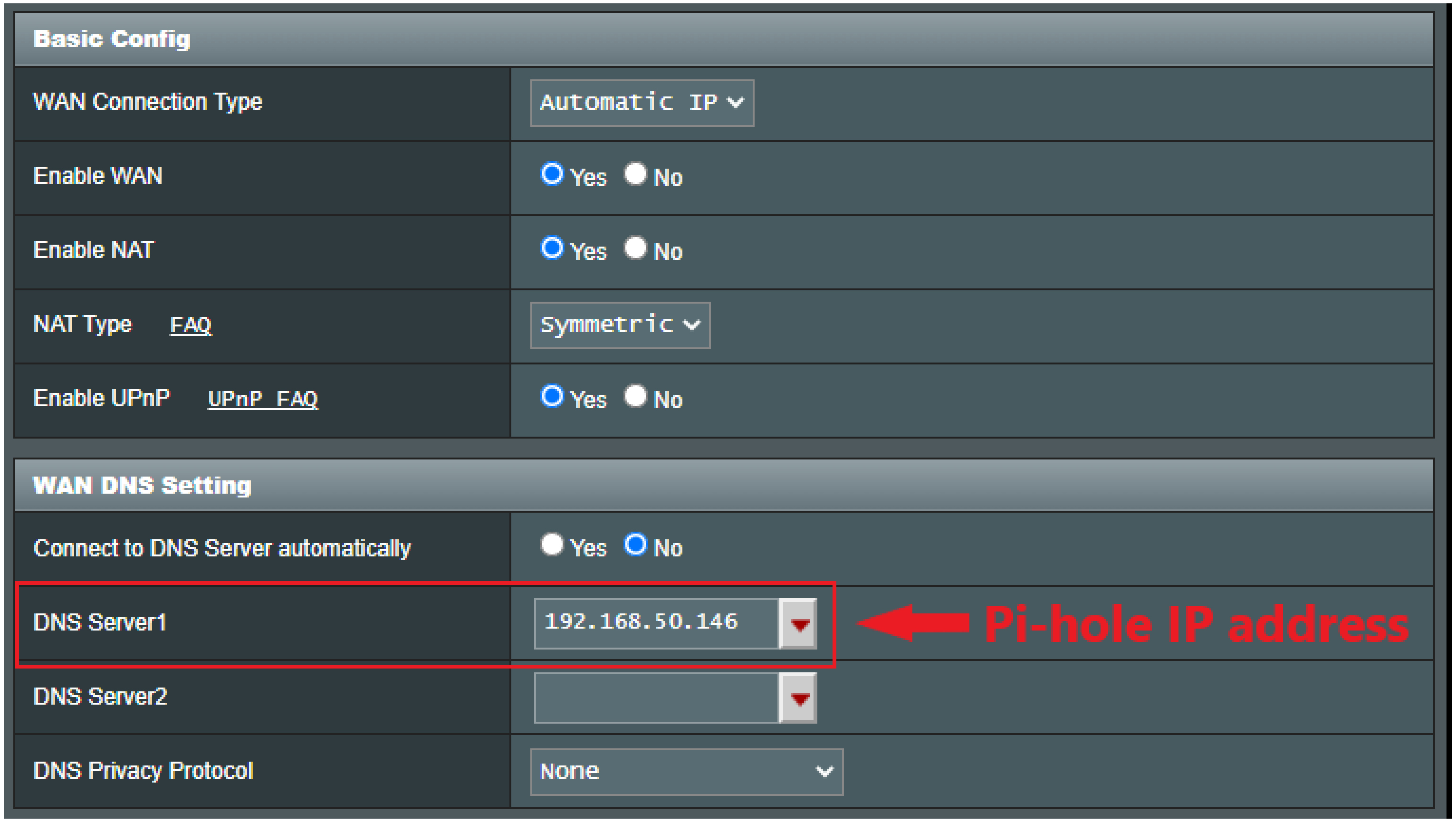
LAN 2

If you have any with NAS settings, please consult your NAS manufacturer.

You can also visit router WEB GUI to check NAS IP address. For more info, please refer to this FAQ: [Wireless Router] How to check the information of devices connected to ASUS router?

Step 4 Enter ASUS router Web GUI. Put NAS IP address in [**WAN**] -> [**Internet Connection**] -> [**WAN DNS Setting**] -> [**DNS Server1**].

Notice：Pi-hole DNS settings may be in WAN or LAN, please refer to your firmware version to set up. For more info, please refer to this FAQ: [Wireless Router] How to configure Router to use Pi-Hole?



Basic Config

WAN Connection Type	Automatic IP
Enable WAN	● Yes ○ No
Enable NAT	● Yes ○ No
NAT Type FAQ	Symmetric
Enable UPnP UPnP FAQ	● Yes ○ No

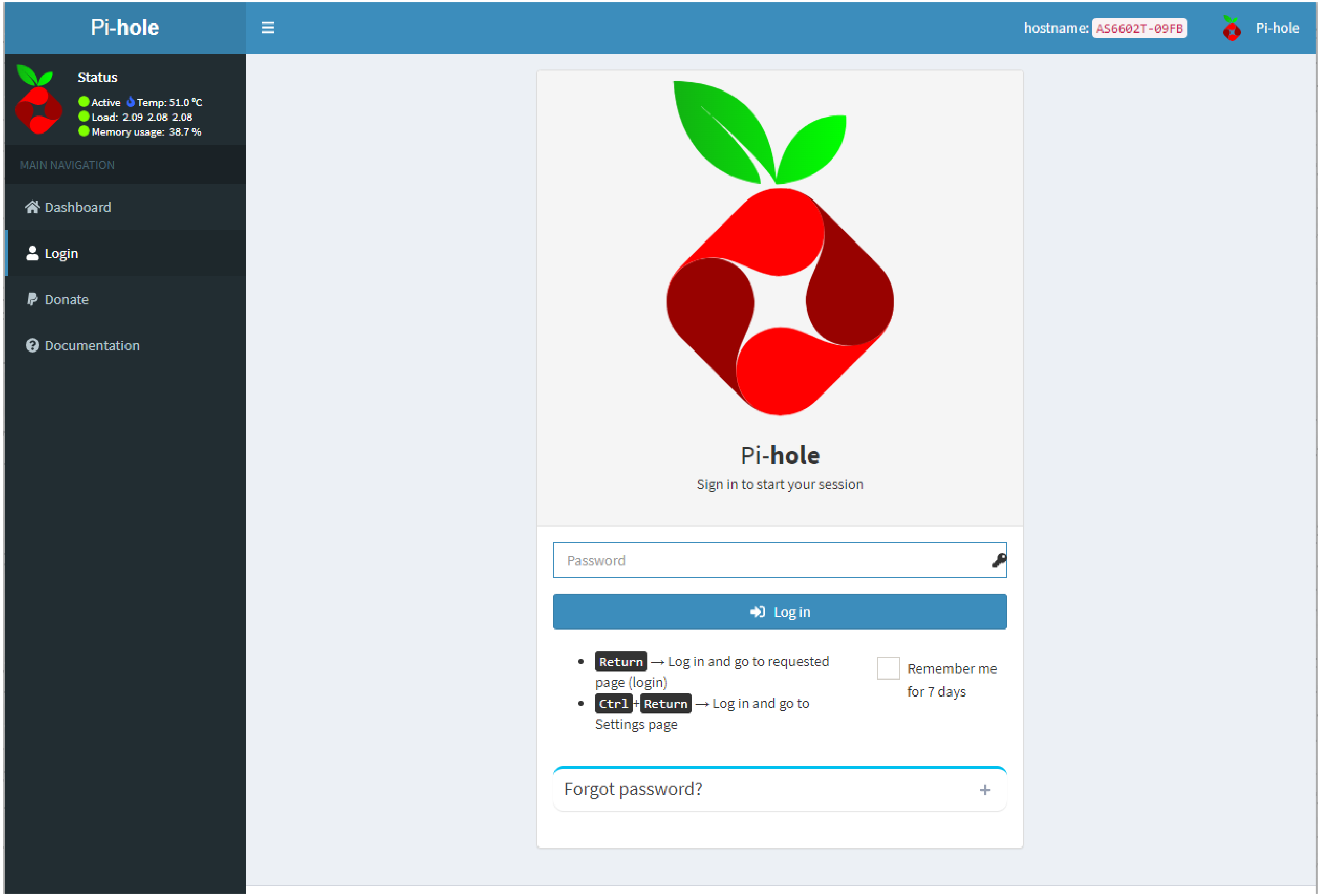
WAN DNS Setting

Connect to DNS Server automatically	○ Yes ● No
DNS Server1	192.168.50.146
DNS Server2	
DNS Privacy Protocol	None

Pi-hole IP address

Note: Please refer to [Wireless Router] How to enter the router's GUI to learn more.

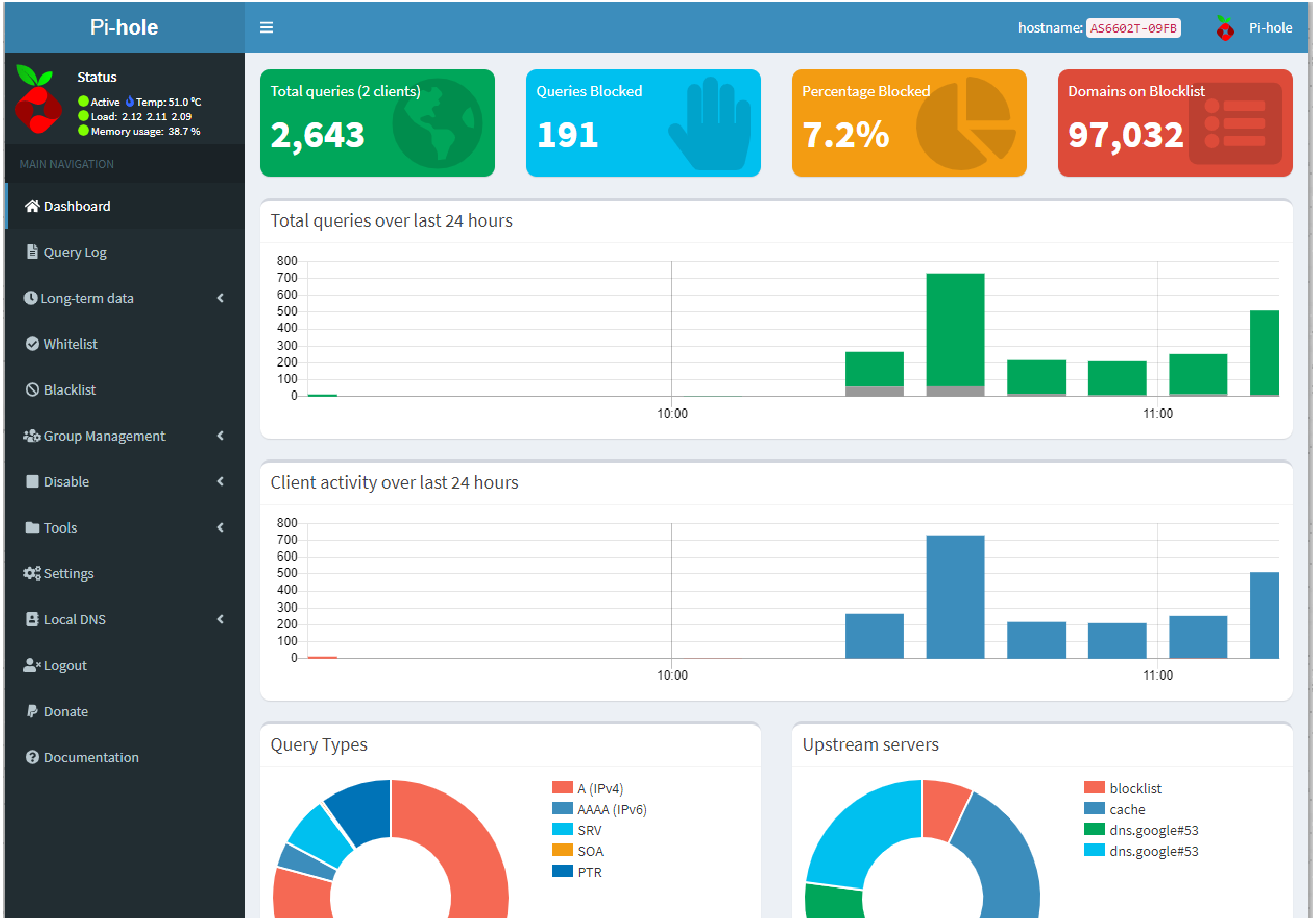
Step 5 Login Pi-hole® on NAS.



- Return → Log in and go to requested page (login)
- Ctrl + Return → Log in and go to Settings page

□ Remember me for 7 days

Forgot password? +



Pi-hole

hostname: AS6602T-09FB

Status
Active Temp: 51.0 °C
Load: 2.12 2.11 2.09
Memory usage: 38.7 %

Total queries (2 clients) 2,643

Queries Blocked 191

Percentage Blocked 7.2%

Domains on Blocklist 97,032

Total queries over last 24 hours

Client activity over last 24 hours

Query Types

Upstream servers

For more information, please refer to : https://pi-hole.net/

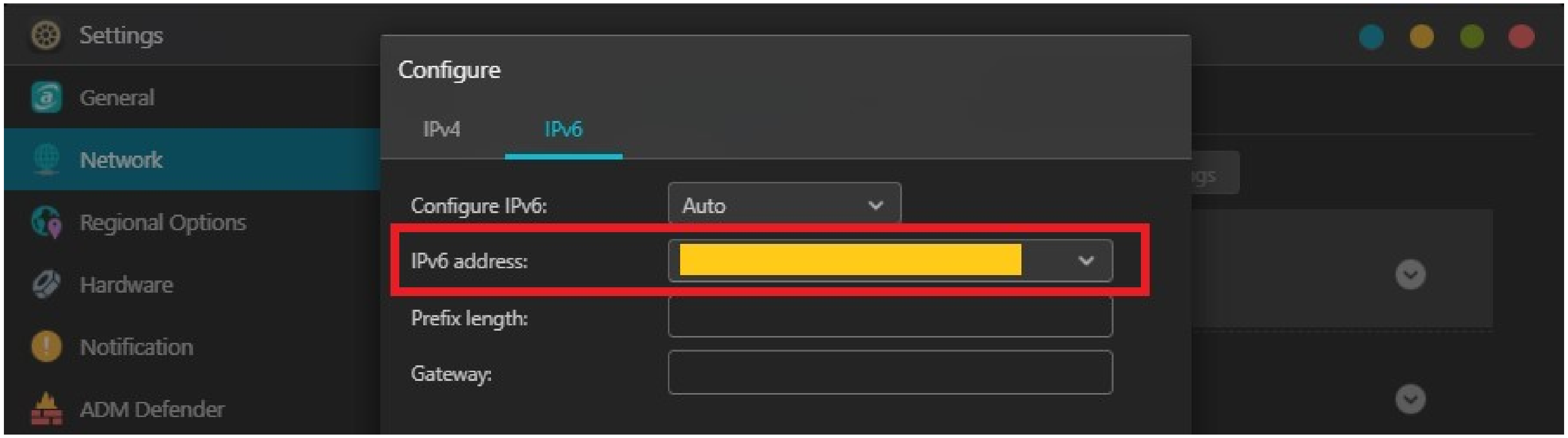
FAQ

1. How to set up IPv6 for Pi-hole®?

If your ISP, Pi-Hole services, and ASUS router all support IPv6, you can set up Pi-hole® DNS server by IPv6 address.

We use ASUS NAS AS6604T for example.

(1)Select [**Settings**] -> [**Network**] -> [**Network interface**] and select the LAN port depending on your connection. Click [**Configure**] -> [**IPv6**] and find your IPv6 address.



Configure IPv6: Auto

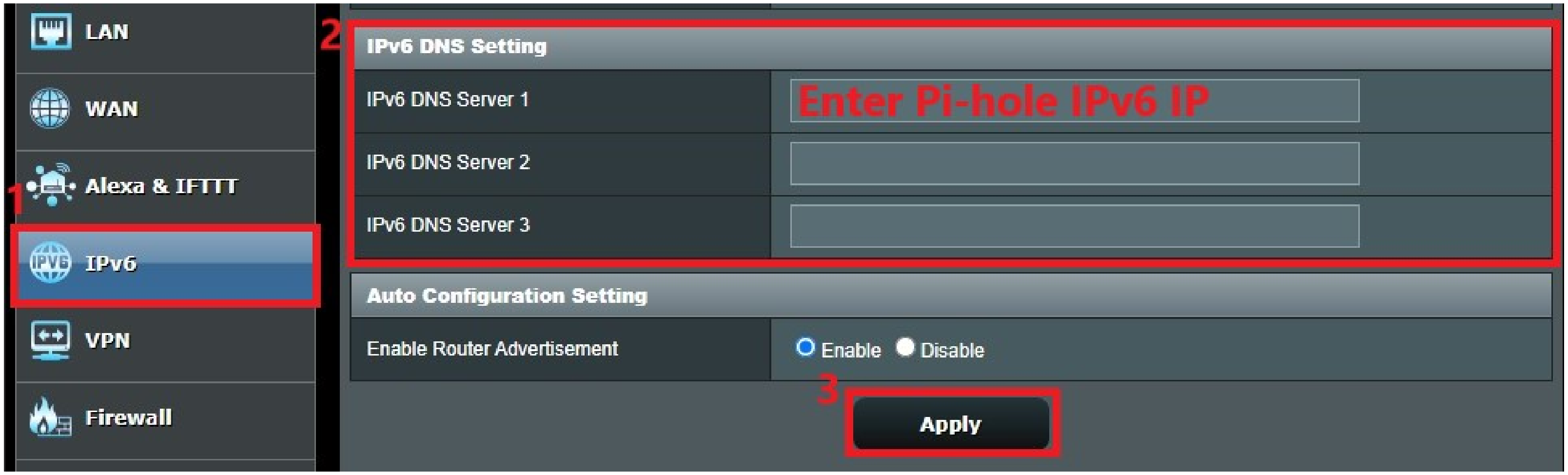
IPv6 address: [redacted]

Prefix length:

Gateway:

(2)Enter router WEB GUI and enable [IPv6]

(3)Put IPv6 address in IPv6 DNS server 1 and click [**Apply**]



IPv6 DNS Setting

IPv6 DNS Server 1: Enter Pi-hole IPv6 IP

IPv6 DNS Server 2

IPv6 DNS Server 3

Auto Configuration Setting

Enable Router Advertisement: ● Enable ○ Disable

For more info, please refer to this FAQ: [IPv6] How to set up IPv6 in ASUS Router?

How to get the (Utility / Firmware)?

You can download the latest drivers, software, firmware and user manuals in the ASUS Download Center.

If you need more information about the ASUS Download Center, please refer this link.

Was this information helpful?

YES NO

Contact Support

If you need more help, see our solutions to get support.

See support

- Above information might be partly or entirely quoted from exterior websites or sources. please refer to the information based on the source that we noted. Please directly contact or inquire the sources if there is any further question and note that ASUS is neither relevant nor responsible for its content/service
- This information may not suitable for all the products from the same category/series. Some of the screen shots and operations could be different from the software versions.
- ASUS provides the above information for reference only. If you have any questions about the content, please contact the above product vendor directly. Please note that ASUS is not responsible for the content or service provided by the above product vendor.
- Brand and product names mentioned are trademarks of their respective companies.

Monitors

Graphics Cards

Show All Products

Accessibility Policy

Terms of Use Notice | Privacy Policy

Canada / English